PLAN DU SOUS SAVOIR S35

Chapitre	Page
A. Les menaces sur les réseaux modernes de données.	2
B. Les firewalls et les IPS	5
C. Les listes de contrôle d’accès.	10
D. Les ACL pour se prémunir de l'IP SPOOFING.	14
E. Sécurisation des commutateurs CATALYST CISCO	18
F. Sécurisation des routeurs CISCO.	26
G. Présentation et configuration d'AAA.	29
H. Les réseaux VPN.	31

A. LES MENACES SUR LES RESEAUX MODERNES DE DONNEES

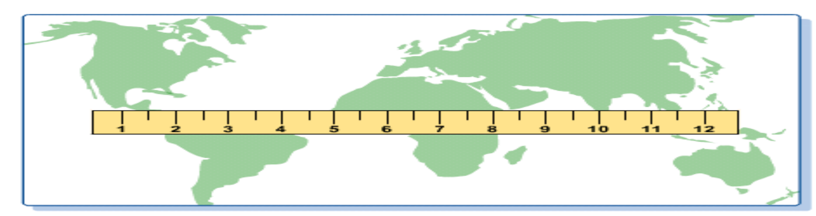
I. Introduction et menaces communes aux réseaux informatiques.

1. Définition.

La sécurité des systèmes informatiques est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires pour conserver ou rétablir la disponibilité, l'intégrité et la confidentialité des informations ou du système.

La sécurité informatique vise généralement cinq principaux objectifs :

- **La confidentialité :** qui consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.
- **L'intégrité** : consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).
- **La disponibilité :** dont l'objectif est de garantir l'accès à un service ou à des ressources.
- **La non-répudiation :** est la garantie qu'aucun des correspondants ne pourra nier la transaction.
- **L'authentification :** consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.



La sécurité d'un réseau est essentielle car Internet a rendu les ordinateurs en réseau accessibles et vulnérables.

Les menaces et risques liés aux réseaux peuvent être classés en :

- Interception qui vise la confidentialité des informations
- Modification qui vise l'intégrité des informations
- Interruption qui vise la disponibilité des informations
- Fabrication qui vise la non-répudiation et l'authentification

2. Evaluation des risques et menaces

La sécurité informatique vise à se protéger contre les risques liés à l'informatique, pouvant être fonction de plusieurs éléments :

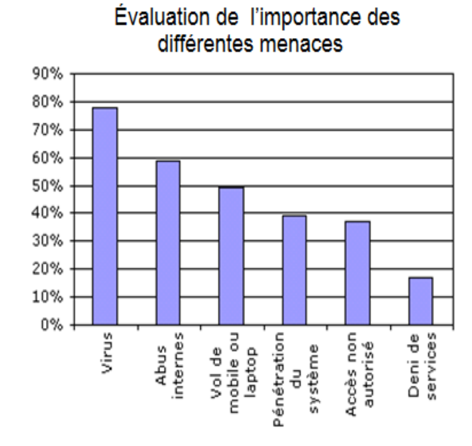
- les **menaces** qui pèsent sur les actifs à protéger ;
- les **vulnérabilités** de ces actifs ;
- les **contre-mesures** ou les remèdes.

Si l'un des éléments est nul, le risque est nul ou infini. C'est pourquoi, l'équation est généralement représentée par :

$$\text{Risques} = \frac{\text{Menaces} * \text{Vulnérabilités}}{\text{Contre-mesures}}$$

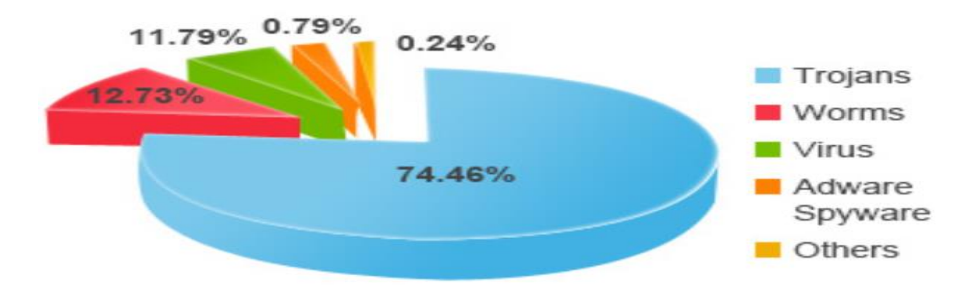
Les principales menaces effectives auxquelles on peut être confronté sont :

- **l'utilisateur** : l'énorme majorité des problèmes liés à la sécurité d'un système d'information est l'utilisateur (par insouciance ou malveillance)
- les **programmes malveillants** : un logiciel destiné à nuire ou à abuser des ressources du système est installé (par négligence ou par malveillance) sur le système, ouvrant la porte à des intrusions ou modifiant les données
- **l'intrusion** : une personne parvient à accéder à des données ou à des programmes auxquels elle n'est pas censée avoir accès
- un **sinistre** (vol, incendie, dégât des eaux) : une mauvaise manipulation ou une malveillance entraînant une perte de matériel et/ou de données.



II. Chevaux de troie, Vers et Virus

Un logiciel malveillant ou maliciel (en anglais : Malware) est un programme développé dans le but de nuire à un système informatique sans accord de l'utilisateur dont l'ordinateur est infecté.
De nos jours, le terme « virus » est souvent employé, à tort, pour désigner toutes sortes de logiciels malveillants. En effet, les maliciels englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces.
La figure suivante donne une évaluation du nombre des plus importants « Malwares »



Chevaux de Troie « Trojans » : sont des programmes qui usurpent l'identité d'autres programmes afin d'obtenir des informations. Par exemple, un cheval de Troie peut émuler l'écran de connexion du système. Lorsque les utilisateurs saisissent leur nom d'utilisateur et leur mot de passe, les informations sont stockées ou transmises au créateur du cheval de Troie. Ces données lui permettent ensuite d'accéder au système.

Vers « Worms » : le ver est un virus autoreproducteur qui n'endommage pas les fichiers mais adopte domicile dans la mémoire active et se reproduit. Les vers utilisent certaines parties automatiques et souvent invisibles d'un système d'exploitation. Bien souvent, leur présence ne peut être détectée que lorsque leur développement est tellement important qu'il nuit aux performances en consommant une grande quantité de ressources système, et en ralentissant ou en interrompant les autres tâches.

Virus : est un petit programme ou code de programme existant à l'intérieur d'autres programmes. Il a des conséquences inattendues et souvent gênantes. Un virus est souvent conçu pour se propager automatiquement vers les autres ordinateurs. Ils peuvent être transmis dans des pièces jointes d'e-mails, lors de téléchargements, ou via une mémoire USB. Certains effets des virus se font sentir dès l'exécution des codes. D'autres virus restent inactifs jusqu'à ce que certaines circonstances en déclenchent l'exécution. Certains virus relèvent seulement du canular. En revanche, d'autres sont dangereux, supprimant des données ou endommageant le système.

Publiciel et espiogiciel « Adware et Spyware » : au moment de la navigation sur le Web, divers programmes sont installés sur l'ordinateur avec ou sans l'accord de l'utilisateur. Ils sont plus communément connus sous leurs terminologies anglaises d'***adware*** et de **spyware.**

- Un **adware** (Advertising Supported Software) est un logiciel qui permet d'afficher des bannières publicitaires. La plupart des annonceurs sont juridiquement légitimes et leur société commerciale reconnue. Les programmes ne diffusent pas d'information vers l'extérieur mais permettent la planification ciblée de messages.
- Les **spywares** sont des adwares qui installent sur le poste de l'utilisateur un logiciel espion et envoient régulièrement et, sans accord préalable, des informations statistiques sur les habitudes de celui-ci. Certains spywares ne se contentent pas de diffuser de l'information. Ils modifient les paramètres système à leur avantage pour imposer, à l'utilisateur qui en est la victime, un certain mode de navigation sur le Web. Ces logiciels peuvent aussi capturer vos habitudes en consultation hors ligne. Ils expédient les résultats de leur collecte à chaque ouverture du navigateur.

L'organisation de l'activité et le bon fonctionnement du système d'information peuvent également être perturbés par la diffusion de courriers ou d'éléments non sollicités tels que :

- des farces, en anglais **jokes** : programmes inoffensifs et dédiés, le plus souvent, à l'amusement,
- des courriers non sollicités, en anglais **spam** : messages à caractère commercial s'appuyant éventuellement sur une usurpation d'adresse électronique,
- des arnaques financières tel que le **scam** : messages vous proposant un montage financier attractif derrière lequel se cache une escroquerie qui s'articule autour d'une demande d'avance de fonds de la part de la victime,
- des rumeurs, en anglais **hoaxes** : informations malveillantes et non fondées qui sont diffusées pour inquiéter les destinataires ou compromettre une personne ou un organisme,
- des lettres chaînes : messages s'appuyant sur l'innocence des destinataires faisant appel à la piété, la générosité et/ou la superstition et proposant éventuellement un enrichissement personnel.

III. Les méthodes et dispositifs pour sécuriser un réseau.

1. Politique de sécurité :

La politique de sécurité est l'ensemble des orientations suivies par une organisation (à prendre au sens large) en termes de sécurité. A ce titre, elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.
Cela signifie qu'elle doit être abordée dans un contexte global :

- La sécurité physique, soit la sécurité au niveau des infrastructures matérielles
- La sécurité des systèmes, des BD et des applications,
- La sécurité des réseaux …

Ainsi, il ne revient pas aux administrateurs informatiques de définir les droits d'accès des utilisateurs mais aux responsables hiérarchiques de ces derniers. Le rôle de l'administrateur informatique est donc de faire en sorte que les ressources informatiques et les droits d'accès à celles-ci soient en cohérence avec la politique de sécurité retenue. De plus, étant donné qu'il est le seul à connaître parfaitement le système, il lui revient de faire remonter les informations concernant la sécurité à sa direction, éventuellement de le conseiller sur les stratégies à mettre en œuvre, ainsi que d'être le point d'entrée concernant la communication aux utilisateurs des problèmes et recommandations en terme de sécurité.

2. Méthodes pour sécuriser les réseaux :

Plusieurs méthodes sont utilisées pour sécuriser les réseaux, on distingue ainsi :

- Authentification : Authentifier un acteur peut se faire en utilisant une ou plusieurs de ses éléments :
  - Ce qu'il sait. Par ex. : votre mot de passe, la date anniversaire de votre grand-mère
  - Ce qu'il a. Par ex. : une carte à puce
  - Ce qu'il est. Par ex. : la biométrie (empreinte digitale, oculaire ou vocale)
- Contrôle d'accès : vérifie les droits d'accès d'un acteur aux données. N'empêche pas l'exploitation d'une vulnérabilité.
- Contrôle d'accès aux communications : le moyen de communication n'est utilisé que par des acteurs autorisés par VPN ou tunnels.
- Contrôle du routage : sécurisation des chemins (liens et équipements d'interconnexion).
- Chiffrement des données : algorithme généralement basé sur des clefs et transformant les données. Sa sécurité est dépendante du niveau de sécurité des clefs. Le chiffrement garantie la confidentialité des données.
- Distribution de clés : distribution sécurisée des clés entre les entités concernées.
- Signature numérique: données ajoutées pour vérifier l'intégrité ou l'origine des données.
- Certification : c'est la preuve d'un fait ou d'un droit accordé. Utilisation d'un tiers de confiance pour l'assurer .
- Horodatage : marquage sécurisé des instants significatifs.

3. Dispositifs pour sécuriser un réseau.

Plusieurs dispositifs logiciel ou matériel sont utilisés pour sécuriser les réseaux, on distingue ainsi :

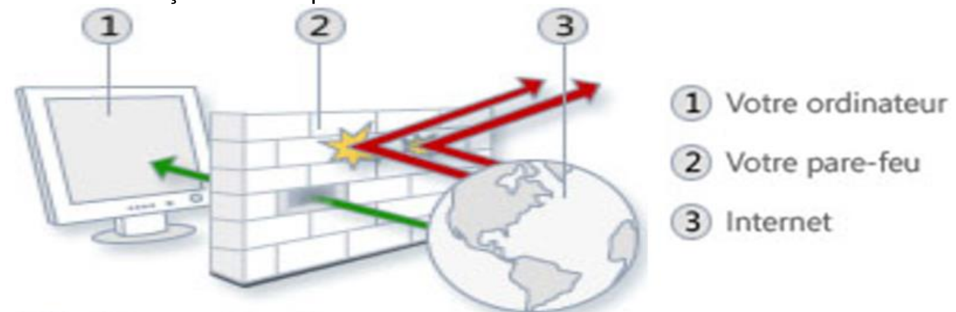
- La protection physique : peut fournir une protection totale, mais qui peut être exagérée. Par ex. isoler complètement son système est une solution qui peut être trop radicale.
- Antivirus : logiciel censé protéger l'ordinateur contre les logiciels (ou fichiers potentiellement exécutables) néfastes. Ne protège pas contre un intrus qui emploie un logiciel légitime, ou contre un utilisateur légitime qui accède à une ressource alors qu'il n'est pas autorisé à le faire.
- Le pare-feu : un élément du réseau informatique contrôlant les communications qui le traversent. Il a pour fonction de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les communications autorisés ou interdites. N'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système. Ne protège pas contre une attaque venant du réseau intérieur (qui ne le traverse pas).
- Détection d'intrusion : repère les activités anormales ou suspectes sur le réseau surveillé. Ne détecte pas les accès incorrects mais autorisés par un utilisateur légitime.
- Journalisation ("logs") : Enregistrement des activités de chaque acteur. Permet de constater que des attaques ont eu lieu, de les analyser et potentiellement de faire en sorte qu'elles ne se reproduisent pas.
- Analyse des vulnérabilités ("security audit") : identification des points de vulnérabilité du système. Ne détecte pas les attaques ayant déjà eu lieu, ou lorsqu'elles auront lieu.

B. LES FIREWALL ET LES IPS

I. Fonctionnement d'un système pare-feu (firewall)

1. Définitions

Un pare-feu est un logiciel ou un matériel qui vérifie les informations provenant d'Internet ou d'un réseau, puis les empêche d'accéder à l'ordinateur ou les y autorise, selon vos paramètres de pare-feu définis.
Le schéma suivant illustre la façon dont un pare-feu fonctionne.



À l'image d'un mur en brique capable de créer un obstacle physique, un pare-feu crée un obstacle entre Internet et votre ordinateur.
Un pare-feu n'est pas la même chose qu'un antivirus. Pour protéger votre ordinateur, vous devez disposer d'un pare-feu et d'un logiciel antivirus contre les programmes malveillants.
Dans le cas où le système pare-feu est fourni dans une boîte noire « clé en main », on utilise le terme d'« appliance ».

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

- D'autoriser la connexion (*allow*) ;
- De bloquer la connexion (*deny*) ;
- De rejeter la demande de connexion sans avertir l'émetteur (*drop*).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la **politique de sécurité** adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- **soit d'autoriser uniquement les communications ayant été explicitement autorisées.**
- **soit d'empêcher les échanges qui ont été explicitement interdits.**

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

2. Filtrage de paquets

Le filtrage simple de paquets :

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets (en anglais « *stateless packet filtering* »). Il analyse les en-têtes de chaque paquet de données (*datagramme*) échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangées entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants :

- adresse IP de la machine émettrice ;
- adresse IP de la machine réceptrice ;
- type de paquet (TCP, UDP, etc.) ;
- numéro de port (rappel: un port est un numéro associé à un service ou une application réseau).

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.
Le tableau ci-dessous donne des exemples de règles de pare-feu :

Règle	Action	IP source	IP dest	Protocol	Port source	Port dest
1	Accept	192.168.10.20	194.154.192.3	tcp	any	25
2	Accept	any	192.168.10.3	tcp	any	80
3	Accept	192.168.10.0/24	any	tcp	any	80
4	Deny	any	any	any	any	any

Les ports reconnus (dont le numéro est compris entre 0 et 1023) sont associés à des services courants (les ports 25 et 110 sont par exemple associés au courrier électronique, et le port 80 au Web). La plupart des dispositifs pare-feu sont au minimum configurés de manière à filtrer les communications selon le port utilisé. Il est généralement conseillé de bloquer tous les ports qui ne sont pas indispensables.

Le filtrage dynamique

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI. Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. Le filtrage dynamique est ainsi capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre côté du pare-feu; l'ensemble des paquets transitant dans le cadre de cette session seront implicitement acceptés par le pare-feu.

Le filtrage applicatif

Le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 (couche application) du modèle OSI, contrairement au filtrage de paquets simple (niveau 4). Le filtrage applicatif suppose donc une bonne connaissance des applications présentes sur le réseau, et notamment de la manière dont elle structure les données échangées (ports, etc.).
Il s'agit d'un dispositif performant, assurant une bonne protection du réseau et une analyse fine des données applicatives ce qui requiert une grande puissance de calcul et se traduit donc souvent par un ralentissement des communications, chaque paquet devant être finement analysé.

3. Les limites des firewalls

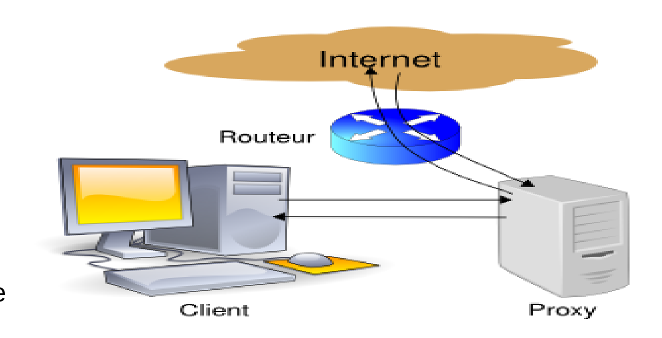
Un système pare-feu n'offre bien évidemment pas une sécurité absolue, bien au contraire. Les firewalls n'offrent une protection que dans la mesure où :

- l'ensemble des communications vers l'extérieur passe systématiquement par leur intermédiaire et qu'ils sont correctement configurés. Ainsi, les accès au réseau extérieur par contournement du firewall sont autant de failles de sécurité. C'est notamment le cas des connexions effectuées à partir du réseau interne à l'aide d'un modem ou de tout moyen de connexion échappant au contrôle du pare-feu.
- l'introduction de supports de stockage provenant de l'extérieur sur des machines internes au réseau ou bien d'ordinateurs portables peut porter beaucoup de dégâts à la politique de sécurité globale.

Enfin, afin de garantir un niveau de protection maximal, il est nécessaire d'administrer le pare-feu et notamment de surveiller son journal d'activité afin d'être en mesure de détecter les tentatives d'intrusion et les anomalies. Par ailleurs, il est recommandé d'effectuer une veille de sécurité (en s'abonnant aux alertes de sécurité des CERT (Computer Emergency Response Team) par exemple) afin de modifier le paramétrage de son dispositif en fonction de la publication des alertes.

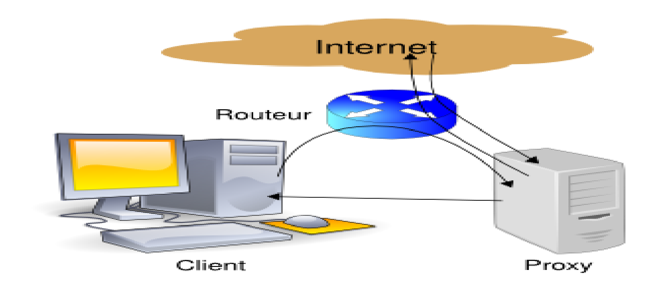
II. Fonctionnement d'un service proxy

Contrairement aux firewalls, qui autorisent ou interdisent une connexion ; le serveur proxy ouvre une connexion à la place du client et peut ainsi lui servir de cache web, on distingue deux types de proxy.



Dans le cas d'un proxy « normal », le client demande au proxy d'interroger le serveur cible. Ce dernier répond au proxy qui communique alors la réponse au client. Dans ce mode, le client est configuré pour utiliser un proxy et il modifie les requêtes http en fonction.

Dans le cas du proxy transparent, le client ignore l'existence du proxy. Il croit envoyer ses requêtes directement au serveur cible, mais ses requêtes sont détournées vers le proxy par le routeur. Le serveur cible répond au proxy qui retransmet la réponse au client, mais ce dernier croit l'avoir reçue directement du serveur cible.



III. Zone DMZ (Zone démilitarisée)

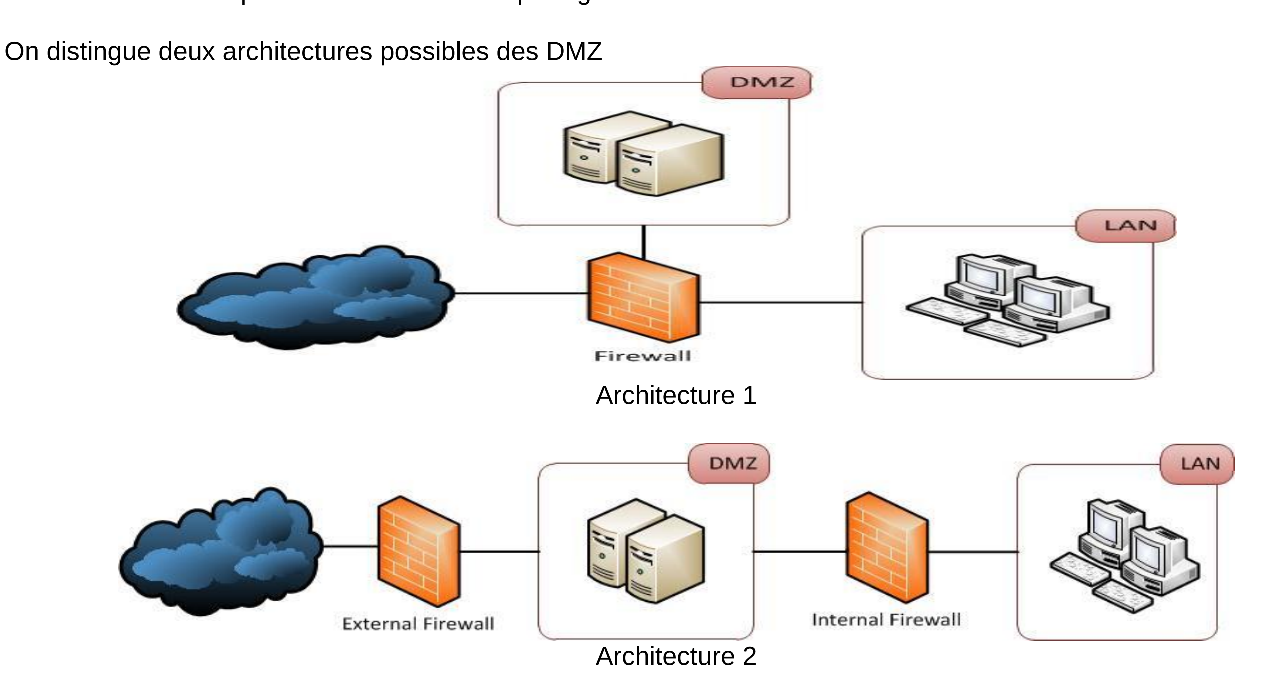
1. Notion de cloisonnement

Les systèmes pare-feu (firewall) permettent de définir des règles d'accès entre deux réseaux. Néanmoins, dans la pratique, les entreprises ont généralement plusieurs sous-réseaux avec des politiques de sécurité différentes. C'est la raison pour laquelle il est nécessaire de mettre en place des architectures de systèmes pare-feux permettant d'isoler les différents réseaux de l'entreprise : on parle ainsi de « **cloisonnement des réseaux** »

2. Architectures DMZ

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de « **zone démilitarisé** » (notée **DMZ** pour *DeMilitarized Zone*) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile.

On distingue deux architectures possibles des DMZ



Architecture 1

Architecture 2

Les serveurs situés dans la DMZ sont appelés « **bastions** » en raison de leur position d'avant poste dans le réseau de l'entreprise.
La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

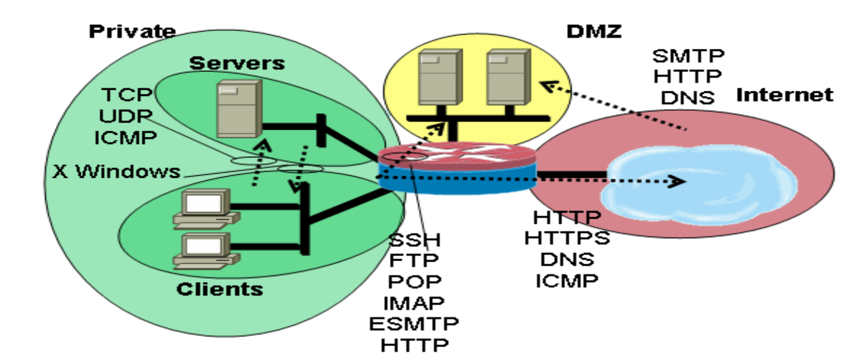
- Trafic du réseau externe vers la DMZ autorisé ;
- Trafic du réseau externe vers le réseau interne interdit ;
- Trafic du réseau interne vers la DMZ autorisé ;
- Trafic du réseau interne vers le réseau externe autorisé ;
- Trafic de la DMZ vers le réseau interne interdit ;
- Trafic de la DMZ vers le réseau externe refusé.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise.

IV. Présentation des firewall Cisco

1. Zone Based Firewall

Sur les anciens modèles de firewall il fallait définir autant d'ACL que l'on avait d'interfaces utilisées pour le firewall. Avec les nouveaux modèles, le principe est de regrouper les interfaces sous forme de zones, et de spécifier quel type de trafic peut passer d'une zone à une autre.



Ce qui est nouveau:

- Application des politiques de sécurité entre les zones, pas par interfaces (une zone peut être constituée d'une ou plusieurs interfaces)
- Il y a une politiques deny all par défaut (donc pas besoin d'ACL).
- On peut, via l'utilisation de classmap, spécifier des politiques différentes par host et par subnet, ou par protocoles

Par défaut, le trafic sera supprimé entre:

- Une interface membre d'une zone vers une interface membre d'une autre zone
- Une interface membre d'une zone vers une interface non membre d'aucune zone

Et le trafic sera autorisé entre:

- Deux interfaces d'une même zone
- Deux interfaces ne faisant partie d'aucune zone (comportement normal, sauf ACL)
- D'une interface membre d'une zone ou non vers le routeur

D'une zone à l'autre, trois actions peuvent être prises:

- Pass : Le trafic est autorisé à transiter d'une zone à l'autre
- Inspect : Autoriser le trafic et inspecter le trafic retour (= ip inspect)
- Drop : Supprimer le trafic

2. Cisco Self Defending Infrastructure

La stratégie «Self-Defending Networks» permet d'assurer la continuité de l'activité de l'entreprise ce qui impose d'appréhender la sécurité au travers d'une approche globale, d'architecture, et pas simplement de produits.

Cisco a développé l'architecture "Self-Defending Networks" pour :

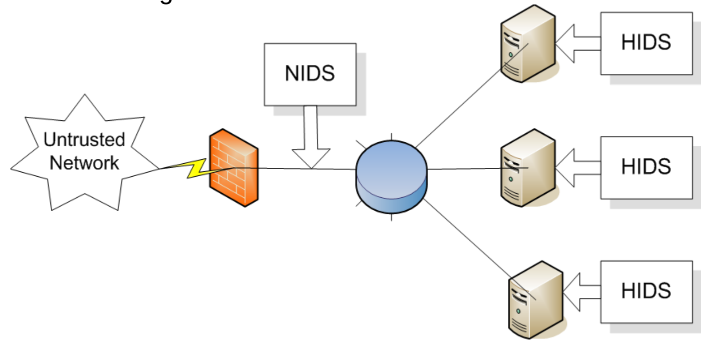
- bloquer les menaces, en intégrant des fonctions de protection du poste, du réseau, du contenu et des applications dans une même infrastructure.
- protéger des dernières menaces, en utilisant des informations récoltées globalement à l'échelle d'internet.
- Pour fournir une protection end-to-end, avec une approche de défense en profondeur



V. Les sondes de détection et de prévention d'intrusion IDS/IPS

1. Les systèmes de détection d'intrusion (HIDS/NIDS)

Les systèmes de détection d'intrusion sont en voie de devenir des composants critiques d'une architecture de sécurité informatique car ils permettent de surveiller, contrôler et détecter les intrusions sur les postes clients ou serveurs et aussi sur le réseau. On distingue ainsi les HIDS et les NIDS.



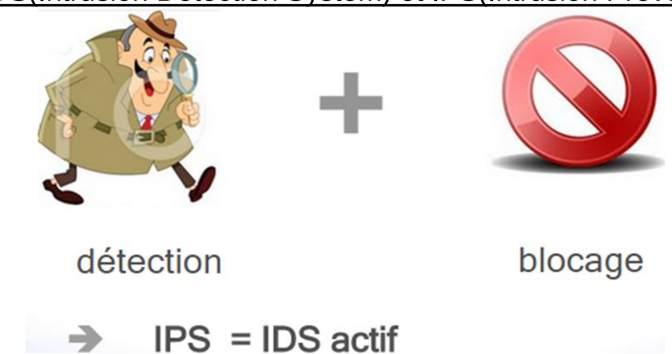
- Système de détection d'intrusion client ou hôte, *Host Intrusion Detection System*, HIDS

Ces utilitaires permettent de détecter une attaque et de vous en informer. Un HIDS analyse tout ce qui se passe sur une station. Il détecte les débordements de droits (obtention du compte root d'une manière suspecte) et d'autres types d'attaques, il contient une base de données sur différentes vulnérabilités.

- Système de détection d'intrusion réseau, Network Intrusion Detection System, NIDS

Un NIDS travaille de la même manière, mais sur les données transitant sur le réseau. Il peut détecter en temps réel une attaque s'effectuant sur l'une de vos machines. Il contient une base de données avec tous les codes malicieux et peut détecter leurs envois sur une des machines. Le NIDS travaille comme un *sniffer* qui analyse automatiquement les flux de données pour détecter une attaque.

2. Différence entre IDS(Intrusion Detection System) et IPS(Intrusion Prevention System)



Alors qu'un IDS se contente de poster une alerte d'intrusion et n'a aucun moyen efficace de la bloquer, un IPS pourra, de par son positionnement en coupure, bloquer une intrusion en temps réel. En fait, les IPS « HIPS et NIPS » ont avant tout été conçus pour lever les limitations des IDS en matière de réponse à des attaques.

Les IPS sont souvent considérés comme des IDS de deuxième génération. Bien qu'il s'agisse d'un abus de langage, cette expression traduit bien le fait que les IPS remplacent petit à petit les IDS.

3. Différence entre IPS et Firewall

Contrairement à un firewall « traditionnel », un IPS se caractérise par les points suivants :

- il doit être complètement furtif. Ceci implique que les interfaces de la sonde ne doivent pas être visibles (pas d'adresse IP, pas d'adresse MAC) et que l'équipement ne doit pas se comporter comme un proxy ou implémenter des mécanismes de manipulation des adresses (comme NAT par exemple)
- l'IPS analyse l'intégralité des paquets en transit, depuis les couches réseaux jusqu'au niveau applicatif.

Il est intéressant de noter qu'il existe très peu d'IPS issus du logiciel libre. Si Snort et Prelude ont fait leurs preuves en matière d'IDS, les projets visant à développer un IPS en logiciel libre (citons Hogwash, Snort-inline) n'ont pas réussi à s'imposer pour le moment.
Du coté des solutions commerciales, les principaux acteurs du marché de l'IPS sont McAfee (IntruShield, Entercept), ISS (Proventia), Juniper (IDP) et 3COM/TippingPoint (Unity One).

C. LES LISTES DE CONTRÔLE D'ACCES

1. Définition

Une liste d'accès ou ACL (Access Control Lists) est un ensemble d'instructions basées sur des protocoles de couche 3 et de couches supérieures pour **filtrer** le trafic. Il s'agit seulement d'appliquer des filtres sur les interfaces afin de bloquer le trafic qui les traverse.
Les ACLs font partie des fonctionnalités de type "firewall" des IOS Cisco.

2. Types de protocoles

Les types de protocoles que nous pouvons configurer dans les instructions de filtrage sont :

- le port source
- l'adresse IP source
- une partie de l'adresse source
- le port de destination
- l'adresse IP de destination
- une partie de l'adresse de destination

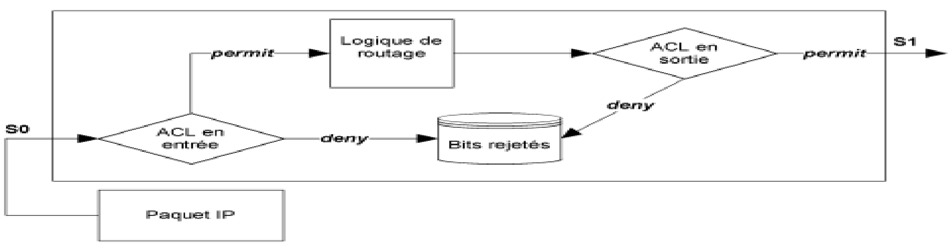
3. Utilité

Une liste d'accès va servir :

- A supprimer des paquets pour des raisons de sécurité (pour du trafic de données ou des accès VTY)
- A filtrer des mises à jour de routage
- A filtrer des paquets en fonction de leur priorité (QoS)
- A définir du trafic intéressant pour des configurations spécifiques

4. Logique

Une liste d'accès, comportant une suite d'instructions de filtrage, va être appliquée sur une interface du routeur, pour le trafic entrant ou pour le trafic sortant. Il va falloir appliquer une logique sur les interfaces en sortie ou en entrée :



5. Caractéristiques

- Les paquets peuvent être filtrés en entrée (quand ils entrent sur une interface) avant la décision de routage
- Les paquets peuvent être filtrés en sortie (avant de quitter une interface) après la décision de routage.
- Le mot clef IOS est "deny" pour signifier que les paquets doivent être filtrés ; précisément les paquets seront refusés selon les critères définis.
- Le mot clef IOS est "permit" pour signifier que les paquets ne doivent pas être filtrés ; précisément les paquets seront permis selon les critères définis.
- **Une instruction implicite rejette tout le trafic à la fin de chaque liste d'accès**

6. Traitement

Le traitement d'une liste d'accès se déroule en deux étapes :

1. Recherche de correspondance (examen de chaque paquet)
2. Action (deny ou permit)

Ensuite ,

3. Si pas de correspondance, instruction suivante
4. Si aucune correspondance, l'instruction implicite est appliquée

7. Différence entre liste d'accès standard et liste d'accès étendue

- Une liste d'accès standard examinera seulement l'adresse IP source.
- Une liste d'accès étendue pourra examiner les adresses IP et les ports aussi bien source que destination, ainsi que le type de protocole (IP, ICMP, TCP, UDP).
- Par ailleurs, il sera possible de vérifier une partie des adresses avec un masque générique (*wildcard mask*).

8. Désignation d'une liste d'accès

On donnera soit un **numéro** ou un **nom** à une liste d'accès (un ensemble d'instructions de filtrage) à appliquer sur une interface en entrée ou en sortie.
Si on utilise un numéro on aura le choix dans une plage de nombres en fonction du protocole de couche 3 :

Protocole	Plage
IP	1 - 99 et 1300 - 1999
IP étendu	100 - 199 et 2000 - 2699
Apple Talk	600 - 699
IPX	800 - 899
IPX étendu	900 - 999
Protocole IPX Service Advertising	1000 - 1099

Si on utilise un nom, il faudra désigner le type de liste : standard ou étendue.

9. Le masque générique (Wildcard Mask)

Il ne faut pas confondre un masque générique (*wilcard mask*) avec un masque de réseau.
Un masque générique est un masque de filtrage.

- Quand un bit aura une valeur de 0 dans le masque, il y aura vérification de ce bit sur l'adresse IP de référence. Lorsque le bit aura une valeur de 1, il n'en y aura pas.
- En binaire, alors qu'un masque de réseau est nécessairement une suite homogène de 1 et puis de 0, un masque générique **peut être** une suite quelconque de 1 et de 0 en fonction du filtrage que l'on veut opérer sur des adresses IP.

Considérons l'exemple suivant :

Adresse de référence :	10.1.1.0	Adresse de référence (binaire) :	00001010. 00000001. 00000001.00000000
Masque générique :	0.0.0.255	Masque générique (binaire) :	00000000. 00000000. 00000000.11111111

En se basant sur le masque en binaire, on peut remarquer que les trois premiers octets de l'adresse de référence doivent correspondre. La valeur du dernier octet n'a pas d'importance. Autrement dit, avec ce masque, toutes les adresses de 10.1.1.0 jusque 10.1.1.255 seront vérifiées.

Voici quelques exemples classiques de masque générique sur n'importe quelle adresse IP :

Masque générique	Version binaire	Description
0.0.0.0	00000000.00000000.00000000.00000000	Tous les bits seront examinés
0.0.0.255	00000000.00000000.00000000.11111111	Les 24 premiers bits seront examinés
0.0.255.255	00000000.00000000.11111111.11111111	Les 16 premiers bits seront examinés
0.255.255.255	00000000.11111111.11111111.11111111	Les 8 premiers bits seront examinés
255.255.255.255	11111111.11111111.11111111.11111111	L'adresse ne sera pas examinée. Tous les bits correspondent d'emblée.
0.0.15.255	00000000.00000000.00001111.11111111	Les 20 premiers bits seront examinés
0.0.3.255	00000000.00000000.00000011.11111111	Les 22 premiers bits seront examinés
32.48.0.255	00100000.00110000.00000000.11111111	Tous les bits seront examinés sauf le 3ème, le 11ème, le 12ème et les 8 derniers

- **Le mot "any" remplace le 0.0.0.0 255.255.255.255, autrement dit toute adresse IP**

- **Le mot "host" remplace le masque 0.0.0.0, par exemple, 10.1.1.1 0.0.0.0 peut être remplacé par "host 10.1.1.1"**

Concrètement, on pourra généraliser de la manière suivante. Le masque générique à utiliser est l'inverse du masque de réseau pour un réseau à filtrer. Par exemple, pour filtrer sur 192.168.1.0/24 (255.255.255.0), on prendra un masque générique 0.0.0.255. Autre exemple aussi, pour filtrer sur 192.168.1.0/27 (255.255.255.224), on prendra un masque générique 0.0.0.31.

10. Règles d'application

- Placer les listes d'accès aussi près que possible de la source des paquets (au niveau de l'interface) s'il s'agit d'une ACL étendue. Par contre, s'il s'agit d'une ACL standard, il faut la placer au plus proche de la destination.
- Placer en tête de liste les règles (les instructions) qui font l'objet d'une correspondance la plus précise et les plus générales à la fin.
- Suivre ces deux recommandations tout en respectant les restrictions d'accès qui ont été identifiées.

11. Syntaxe des commandes

La mise en œuvre d'une ACL se déroule en deux étapes :

- Création de la liste, en plaçant les instructions les unes après les autres suivies d'un retour chariot.
- Application sur une interface en entrée ou en sortie

11.1. Liste d'accès standard

Router(config)#**access-list** *numéro-liste-accès* {**deny|permit**} *adresse-source masque-source*

11.2. Liste d'accès étendue

Router(config)#**access-list** *numéro-liste-accès* {**deny|permit**} *protocole adresse-source masque-source* [*opérateur port*] *adresse-destination masque-destination* [*opérateur port*]

Où : "opérateur" peut prendre les valeurs suivantes :

lt (less than)
gt (greater than)
eq (equal)
neq (not equal)
range (inclusive range).

Où le paramètre "port" peut prendre une valeur nominative ou numéraire de 0 à 65535 ou, par exemple, http, telnet, ftp, etc.

11.3. Liste d'accès nommée

Router(config)#**ip access-list standard** *nom*
Router(config-ext-nacl)#**permit|deny** …
Router(config)#**ip access-list extended** *nom*
Router(config-ext-nacl)#**permit|deny** …

11.4. Activation d'une liste d'accès sur une interface

Router(config-if)#**ip access-group** {*numéro-liste-accès*|*nom* [**in** | **out**]}

11.5. Diagnostic

Router#**show ip interface** [*type numéro*]
Router#**show access-lists** [*numéro-liste-accès*|*nom-liste-accès*]
Router#**show ip access-list** [*numéro-liste-accès*|*nom-liste-accès*]
On pourra "logguer" le comportement d'une ACL en ajoutant le terme **log** à la fin d'une directive. Un **show logging** donnera le résultat.

12. Optimisation du masque générique

Chaque paquet sera vérifié par chaque entrée d'une ACL. Il y aura autant de vérification qu'il y a de paquets et d'entrées. Des listes d'accès trop longues peuvent engager beaucoup de ressources. Il s'agira de les optimiser. Aussi, on peut également élaborer des critères de vérifications assez fins. En voici des exemples.

12.1. Summarization d'ACL

Considérons ces huit réseaux à filtrer :

- 192.168.32.0/24
- 192.168.33.0/24
- 192.168.34.0/24
- 192.168.35.0/24
- 192.168.36.0/24
- 192.168.37.0/24
- 192.168.38.0/24
- 192.168.39.0/24

Les deux premiers octets sont identiques. Ils devront être vérifiés. Le masque générique commencera par 0.0.
Le troisième octet varie. Il peut être écrit comme dans le tableau suivant conformément à la position de chaque bit par rapport à sa valeur :

Décimale	128	64	32	16	8	4	2	1
32	0	0	1	0	0	0	0	0
33	0	0	1	0	0	0	0	1
34	0	0	1	0	0	0	1	0
35	0	0	1	0	0	0	1	1
36	0	0	1	0	0	1	0	0
37	0	0	1	0	0	1	0	1
38	0	0	1	0	0	1	1	0
39	0	0	1	0	0	1	1	1
	M	M	M	M	M	D	D	D

On remarque aisément que les cinq premiers bits correspondent exactement (M) alors que les trois derniers changent (D). Le masque générique sur cet octet sera donc : 7 (00000111)
Dans le cas présenté, le dernier octet ne doit pas être vérifié. Le masque générique sera : 0.0.7.255
Notons que cet ensemble d'adresses peut être résumé avec le masque de super-réseau : "192.168.32.0/21" ou "192.168.32.0 255.255.248.0". Dans ce cas commun dans lequel il faudra vérifier ce groupe d'adresse IP, le masque générique sera l'**inverse** du masque réseau : en soustrayant 255.255.248.0 de 255.255.255.255, on obtient 0.0.7.255

12.2. Filtrage fin

Quelle méthode a été employée pour découvrir les bits qui doivent être filtrés sur une adresse IP ? On a désigné les bits qui ne varient pas d'une adresse à une autre et nous les avons marqué avec un masque générique à la valeur 0 en binaire. Par exemple, pour filtrer sur un octet uniquement les adresses paires :

Décimale	128	64	32	16	8	4	2	1
0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	1	0
4	0	0	0	0	0	1	0	0
6	0	0	0	0	0	1	1	0
8	0	0	0	0	1	0	0	0
10	0	0	0	0	1	0	1	0
x pairs	?	?	?	?	?	?	?	0

On constate que le point commun entre toutes ces adresses ne concerne que le dernier bit de l'octet. C'est donc ce dernier qu'il faudra vérifier par rapport à une adresse de référence. Concrètement, en binaire, on aura un masque sur l'octet de "11111110", "254" en décimale avec comme octet de référence binaire "00000000", "0" en décimale. Avec la directive "192.168.1.0/0.0.0.254", on filtrera toutes les adresses paires du réseau 192.168.1.0/24.
C'est comme si on disait, vérifie :

- que le premier octet soit toujours égal à 192 en décimale,
- que le second octet soit toujours égal à 168 en décimale,
- que le troisième octet soit toujours égal à 1 en décimale,
- que le dernier bit du quatrième octet soit toujours égal à zéro en binaire, soit que sa valeur décimale soit paire.

D. LES ACL POUR SE PRÉMUNIR DE L'IP SPOOFING

1 - LES PRINCIPALES ATTAQUES.

1.1 - Attaque par déni de service (DOS)

Une « **attaque par déni de service** » (en anglais « **Denial of Service** », abrégé en *DoS*) est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à la réputation des sociétés ayant une présence sur Internet.

On distingue habituellement deux types de dénis de service :

- Les dénis de service par saturation, consistant à submerger une machine de requêtes, afin qu'elle ne soit plus capable de répondre aux requêtes réelles ;
- Les dénis de service par exploitation de vulnérabilités, consistant à exploiter une faille du système distant afin de le rendre inutilisable.

Lorsqu'un déni de service est provoqué par plusieurs machines, on parle alors de « **déni de service distribué** » (noté *DDOS* pour *Distributed Denial of Service*).

1.2 - Attaque par empoisonnement ARP (ARP Poisoning)

Cette attaque se base sur l'envoi d'informations ARP falsifiés. Ainsi, les différents équipements du LAN apprennent des mauvaises correspondances adresses IP avec MAC. La conséquence est de rompre toutes communications entre deux équipements IP. Les cibles sont souvent les serveurs, les routeurs et les switch rendant indisponible les services associés.

1.3 - Attaque "Ping de la mort" (Ping of death)

(ping est un outil exploitant le protocole ICMP, permettant de tester les connexions sur un réseau en envoyant un paquet et en attendant la réponse)

L'attaque "Ping de la mort" est dépassée, mais elle a fait ses preuves à l'époque. Elle exploitait une faiblesse dans l'implémentation de la plus part des piles IP en envoyant un paquet ICMP d'une taille non conforme (supérieur à 64 octets). Ceci avait pour effet de planter directement la pile IP attaquée.

1.4 - Attaque "hôte inaccessible" (Unreachable Host)

Cette attaque envoie des messages ICMP de type "Host Unreachable" à une cible, provoquant la déconnexion des sessions et paralyse ainsi la victime. La simplicité de cette attaque est qu'elle ne demande qu'un faible débit du fait que les envois de datagramme ICMP peuvent être sur une faible cadence.

1.5 - Attaque "redirection du ICMP" (ICMP Redirect)

Cette attaque envoi des messages ICMP de type "Redirect" à une cible pouvant être aussi bien un serveur comme un routeur. Le datagramme informera la victime qu'il faut passer par un autre chemin. Ainsi, cela provoquera une indisponibilité WAN.

1.6 - Attaque "inondation avec ping" (Ping Flood ou ICMP Flood)

Beaucoup d'hôte Internet ou privée répondent aux paquets ICMP, il est donc facile de les inonder de ce flux afin les rendre indisponibles. D'ailleurs, que les cibles répondent ou pas à l'ICMP, l'objectif premier étant de saturer leurs bandes passantes d'accès réseau, processeurs, mémoire ...

Ping Flood est la plus répandu des attaques par déni de service, car de nombreux particuliers et amateurs s'amusent simplement à pinguer un host distant. Et bien sûr, ils se font plaisir en ajoutant les options permettant d'augmenter la cadence au maximum. On peut citer dans ce même principe l'attaque "inondation UDP" (UDP Flood).

1.7 - Attaque Land "terre" (Land Attack)

Cette attaque consiste à démarrer une ouverture de session TCP via un SYN à destination d'un port ouvert de la machine cible. L'astuce de l'attaque est de préciser l'adresse IP source identiquement à l'IP destination ainsi que le port source identiquement au port destination. La victime recevant cette trame pense alors qu'il discuter avec lui même ce qui généralement provoquait un crash.

1.8 - Attaque "inondation par des ouvertures de session TCP" (TCP/SYN Flooding)

C'est une attaque par saturation (*déni de service*) exploitant le mécanisme de poignée de main en trois temps (en anglais *Three-ways handshake*) du protocole TCP.

Le mécanisme de poignée de main en trois temps est la manière selon laquelle toute connexion « fiable » à Internet (utilisant le protocole TCP) s'effectue.

Lorsqu'un client établit une connexion à un serveur, le client envoie une requête SYN, le serveur répond alors par un paquet *SYN/ACK* et enfin le client valide la connexion par un paquet *ACK* (*acknowledgement*, qui signifie *accord* ou *remerciement*).

Une connexion TCP ne peut s'établir que lorsque ces 3 étapes ont été franchies. L'attaque SYN consiste à envoyer un grand nombre de requêtes SYN à un hôte avec une adresse IP source inexistante ou invalide. Ainsi, il est impossible que la machine cible reçoive un paquet *ACK*.

Les machines vulnérables aux attaques SYN mettent en file d'attente, dans une structure de données en mémoire, les connexions ainsi ouvertes, et attendent de recevoir un paquet *ACK*. Il existe un mécanisme d'expiration permettant de rejeter les paquets au bout d'un certain délai. Néanmoins, avec un nombre de paquets SYN très important, si les ressources utilisées par la machine cible pour stocker les requêtes en attente sont épuisées, elle risque d'entrer dans un état instable pouvant conduire à un plantage ou un redémarrage.

1.9 - Attaque "détournement de session TCP" (TCP session hijacking)

Le « **vol de session TCP** » (également appelé *détournement de session TCP* ou en anglais *TCP session hijacking*) est une technique consistant à intercepter une session TCP initiée entre deux machines afin de la détourner. Dans la mesure où le contrôle d'authentification s'effectue uniquement à l'ouverture de la session, un pirate réussissant cette attaque parvient à prendre possession de la connexion pendant toute la durée de la session.

1.10 - Attaque Mail Bombing

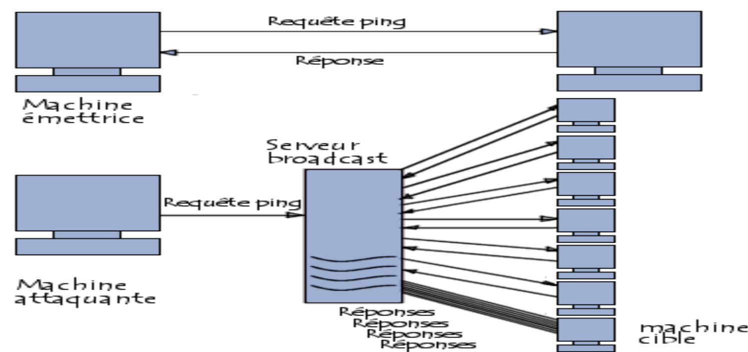
Cette attaque, très souvent utilisée par du grand public, consiste à envoyer plusieurs milliers d'emails à destination d'une entreprise ou d'un utilisateur cible. L'impact est évidement avec un remplissage massif de la boite à lettre utilisateur, mais surtout de saturer le débit Internet de l'entreprise ciblée qui ne possède pas de qualité de service.

1.11 - Attaque par réflexion (smurf attack)

La technique dite « attaque par réflexion » (en anglais « smurf ») est basée sur l'utilisation de serveurs de diffusion (*broadcast*) pour paralyser un réseau. Un serveur broadcast est un serveur capable de dupliquer un message et de l'envoyer à toutes les machines présentes sur le même réseau.

Le scénario d'une telle attaque est le suivant :

- la machine attaquante envoie une requête *ping* à un ou plusieurs serveurs de diffusion en falsifiant l'adresse IP source (adresse à laquelle le serveur doit théoriquement répondre) et en fournissant l'adresse IP d'une machine cible.
- le serveur de diffusion répercute la requête sur l'ensemble du réseau ;
- toutes les machines du réseau envoient une réponse au server de diffusion,
- le serveur broadcast redirige les réponses vers la machine cible.
- Ainsi, lorsque la machine attaquante adresse une requête à plusieurs serveurs de diffusion situés sur des réseaux différents, l'ensemble des réponses des ordinateurs des différents réseaux vont être routées sur la machine cible.



De cette façon l'essentiel du travail de l'attaquant consiste à trouver une liste de serveurs de diffusion et à falsifier l'adresse de réponse afin de les diriger vers la machine cible.

2 – LES LIMITATIONS DES ACL : ATTAQUE PAR USURPATION D'ADRESSE IP (SMART-SPOOFING IP)

2.1 - Le filtrage IP

Le filtrage IP consiste en la mise en place de règles de contrôle d'accès portant sur l'adresse IP source des paquets entrant dans un équipement ou une application, il consiste à comparer l'adresse IP source du paquet entrant avec une liste d'adresses autorisées. Le paquet IP sera accepté seulement si l'adresse fait partie de cette liste. Dans le cas contraire, le paquet sera rejeté (émission d'un refus ou poubellisation).

Le filtrage IP est donc un composant de sécurité de base, simple et performant, que l'on retrouve dans nombre d'équipements et de logiciels :

- Firewall avec utilisation de règles intégrant l'IP source
- Routeurs avec Access List (ACL)
- Filtres intégrés dans les piles IP des systèmes d'exploitation
- Filtrage IP effectué au sein des applications afin de limiter les communications entre deux machines.

2.2 - Le spoofing IP

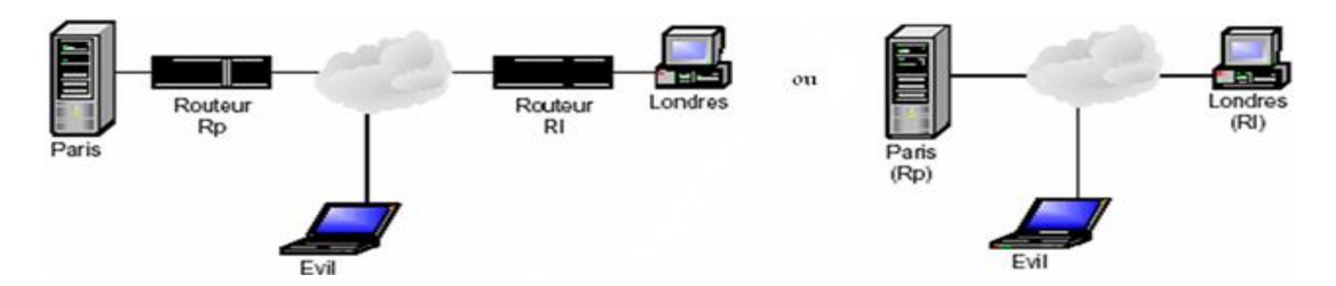
La méthode du spoofing d'IP source permet de contourner ce filtrage. Le concept est simple mais les techniques pour y parvenir sont plus complexes. Il suffit de voler l'adresse IP d'une machine autorisée pour profiter de ses privilèges. Pour y parvenir, seules les techniques basées sur la construction manuelle de paquets IP étaient jusqu'alors connues. Jumelées à de l'écoute réseau, cela permettait au mieux de créer une pseudo communication avec la machine visée.

2.3 - Le smart-spoofing IP

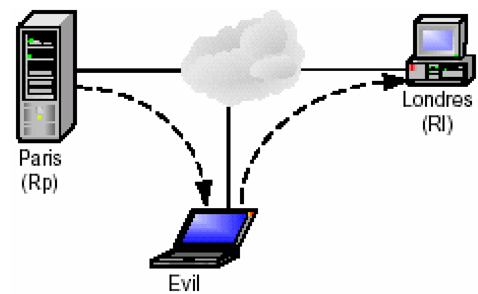
Cette technique abandonne les principes d'écoute du réseau et de forgeage de paquets. Elle permet de spoofer une adresse IP de façon "propre", en permettant à n'importe quelle application exécutée de "profiter" de cette nouvelle identité. Cette méthode a été nommée le "smart-spoofing IP".

Pour expliquer cette attaque, nous appellerons "Paris" la machine sur laquelle le filtrage IP est effectué, "Londres" la machine autorisée à se connecter sur Paris et "Evil" la machine opérant le smart-spoofing IP.

- Evil doit être sur le chemin réseau entre Paris et Londres.
- Deux routeurs Rp et Rl sont positionnés. Ils permettront à Evil de joindre respectivement Paris et Londres. Selon que Evil se situe dans le même réseau que Paris ou Londres, Rp et Rl pourront se confondre avec Paris ou Londres.

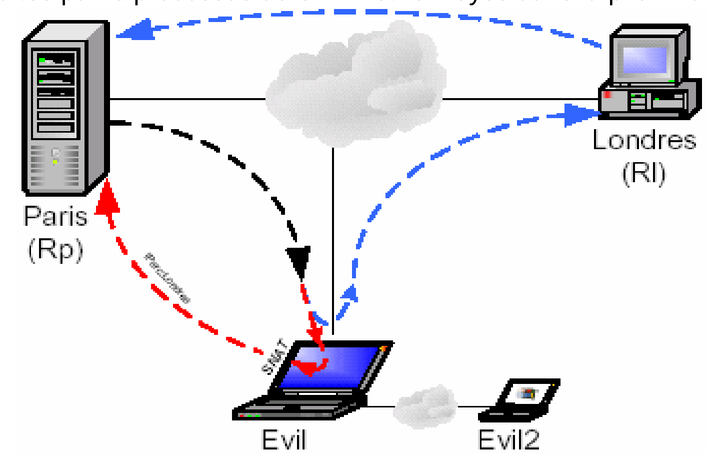


- Le smart-spoofing IP consiste à opérer dans un premier temps un ARP cache poisoning de Rp afin d'insérer Evil dans la chaîne de routage niveau 2 des paquets circulant entre Londres et Paris.
- Il est nécessaire d'activer le routage sur Evil afin que Londres continue à recevoir les paquets qui lui sont destinés.



- Une fois ceci réalisé, l'ensemble des paquets circulant de Paris vers Londres passera par Evil.

- La deuxième étape consiste à mettre en place un mécanisme de translation d'adresse source (SNAT) sur Evil, de sorte que les connexions créées vers Paris le soit avec l'adresse source de Londres. Les paquets en retour seront naturellement traités par le processus de SNAT et renvoyés dans la pile IP de Evil.



- La dernière étape consiste à utiliser le logiciel client de l'application protégée par le filtrage IP source (telnet, browser, ftp, console d'administration...) afin d'accéder à Paris en se faisant passer pour Londres. Le logiciel client peut être exécuté sur Evil lui-même ou sur Evil2, une machine sous Windows située dans un réseau juste derrière Evil.

Il est à noter certaines techniques (par exemple le spoofing DNS) permettant de s'insérer sur un chemin réseau (modification du routage au niveau 3 cette fois ci)

Que vaut réellement une règle de filtrage IP source positionnée sur Paris (qu'il soit un firewall, un routeur, une application...) et n'autorisant que l'adresse IP de Londres ?

Globalement, il faut considérer que la règle en question correspond à autoriser toutes les machines des réseaux situés sur le chemin entre Paris et Londres. Ces machines ont en effet la possibilité d'effectuer un ARP cache poisoning de leur Rp, et donc de se faire passer pour Londres.

2.4 – Comment se protéger ?

- Le filtrage IP n'a jamais été considéré comme unique protection d'accès à un équipement ou une ressource.
- L'accès nécessite généralement une phase d'authentification (par mot de passe...).
- Le VPN est un moyen efficace de protection contre le spoofing IP.
- Le chiffrement permet de supprimer le problème lié à l'écoute sur le réseau.
- Le verrouillage adresses IP/MAC peut aussi éviter le spoofing IP mais limité aux réseaux locaux.

E. SÉCURISATION DES COMMUTATEURS CATALYST CISCO

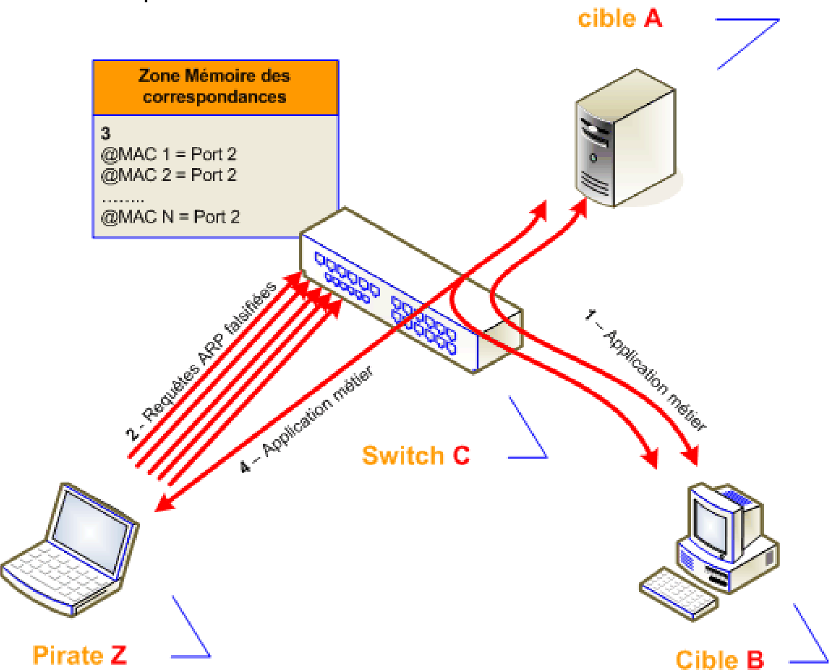
I. LES PRINCIPALES ATTAQUES.

1. Attaque MAC Flooding

Cette attaque est basée sur l'envoi massif de requête et réponse ARP. Chaque requête doit avoir une adresse MAC différente, ainsi les différents Switchs du LAN vont apprendre cette correspondance entre l'adresse MAC et le port physique. Avec un envoi massif, le Switch saturera rapidement sa mémoire qui est limitée. Les conséquences peuvent être multiples comme par exemple :

- Arrêt du fonctionnement du Switch ne pouvant plus commuter de trame
- Passage du Switch en mode HUB permettant ainsi à l'attaquant d'effectuer de l'écoute.

Le schéma ci-dessous montre le procédé :



1 - Les cibles A et B s'échangent des informations normalement
2 - Le pirate Z envoi plein de requêtes ARP avec des adresses MAC différentes
3 - Le Switch C met à jour sa table de correspondance jusqu'à saturation de la mémoire
4 - Les cibles A et B s'échangent des informations, mais le pirate les reçoit aussi du fait que le Switch fonctionne désormais en HUB

Ils existent plusieurs possibilités afin d'éviter cette attaque. Par exemple, il est possible :

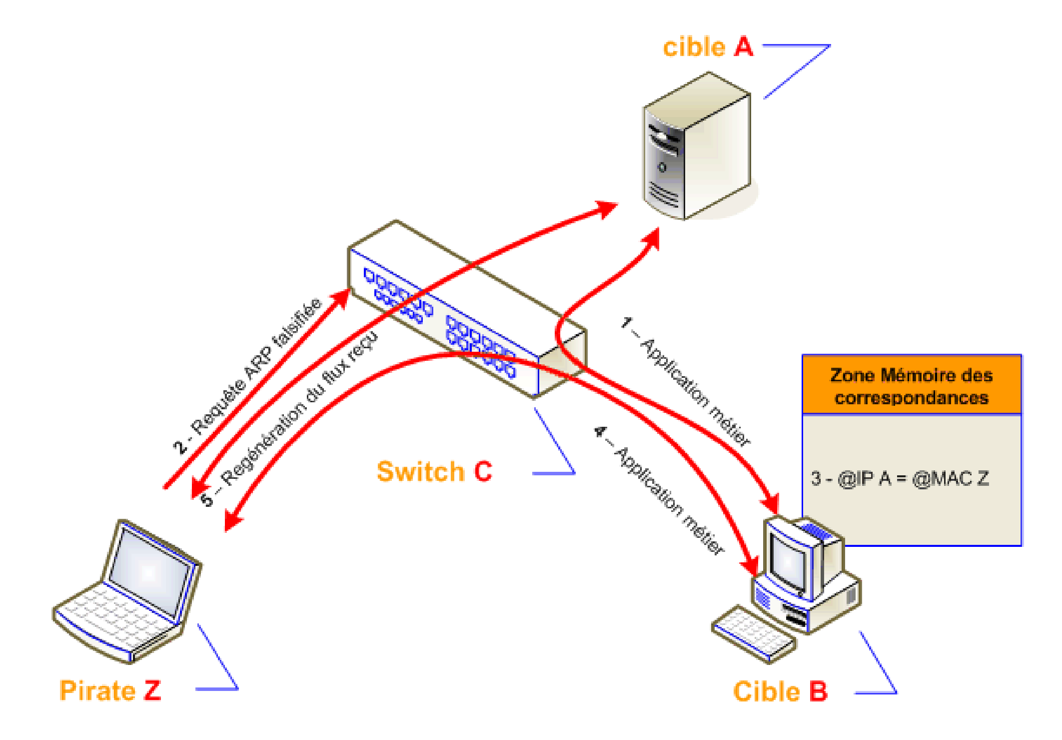
- De n'autoriser qu'une liste d'adresse MAC prédéfinie par port. Cisco propose cela via la commande "switchport port-security mac-address H.H.H"
- D'appliquer un filtre sur le nombre de correspondance maximum par port. 3 modes existent qui sont "protect", "restrict" et "shutdown"
- D'utiliser l'authentification 802.1X

2. Attaque ARP Poisoning

Cette attaque se base sur l'envoi d'informations de requêtes ARP falsifiées. L'intérêt est de faire croire aux autres que l'adresse IP de la cible correspond à une adresse MAC que l'on choisie. Ainsi, les différents équipements du LAN apprennent la mauvaise correspondance.
Les conséquences peuvent être multiples tel que :

- La rupture de toutes communications de la cible IP. Les cibles sont souvent les serveurs et les routeurs rendant indisponible les services associés
- L'écoute des flux de la cible. Pour cela, il faut spécifier l'adresse MAC du hackeur dans l'information ARP.

Le schéma ci-dessous montre le procédé :



1 - Les cibles A et B s'échangent des informations normalement
2 - Le pirate Z envoi une requête ARP empoisonnée
3 - La cible B met à jour sa table de correspondance
4 - La cible B envoi ses donnée au pirate Z en croyant s'adresser à la cible A
5 - La pirate transfert les données reçues vers la cible A en mettant sa réelle adresse MAC source afin de s'assurer de recevoir les réponses

Ils existent plusieurs possibilités afin d'éviter cette attaque. Par exemple, il est possible :

- De n'autoriser qu'une liste d'adresse MAC prédéfinie par port. Cisco propose cela via une commande.
- D'utiliser une détection IDS sur le Switch
- D'utiliser l'authentification 802.1X

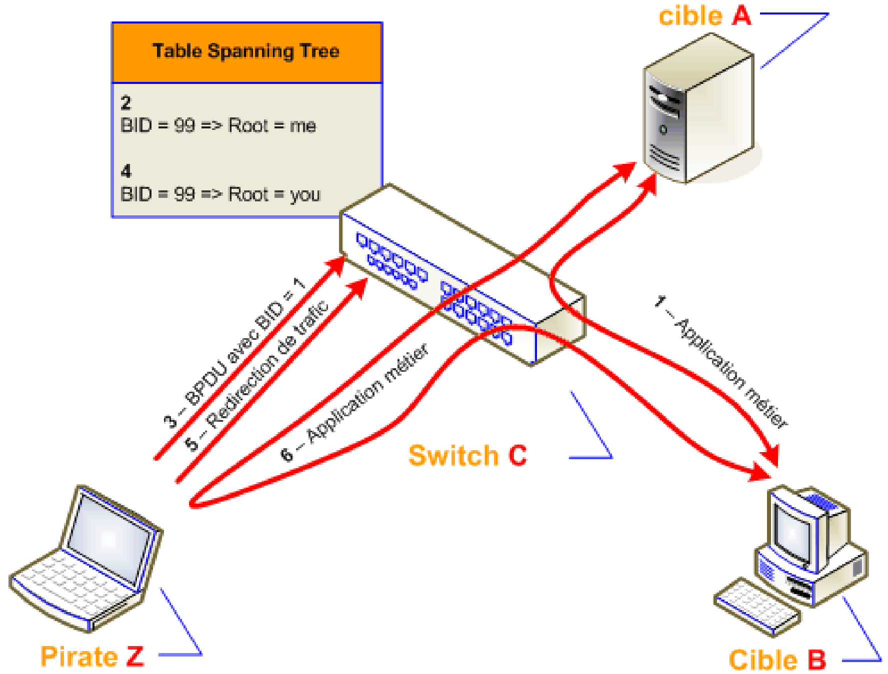
3. Attaque spanning tree

Cette attaque se base sur l'envoi de trames BPDU (bridge protocol data units) à destination du Switch cible. Dans un environnent Sapnning-Tree, il y a un seul Switch qui est élu root (maître) servant de référence pour les coûts et les chemins. Ces trames BPDU émises avec un BID (Bridge ID) très petit, obligera les commutateurs à recalculer le nouveau root.

Cela dépend du constructeur, de l'équipement et de la version, mais les conséquences peuvent être multiples comme par exemple :

- Suite à la saturation processeur provoquée par les calculs permanents, les commutateurs ne commutent plus ou crash littéralement. Il est même possible que les Switchs basculent alors en mode HUB permettant ainsi à l'attaquant d'effectuer de l'écoute.
- Suite à l'envoi d'un BID plus petit que ceux des Switchs, l'attaquant se retrouvera alors élu comme maître de l'environnement Spanning-Tree. Ainsi, le hackeur pourra redéfinir la topologie à sa guise et ainsi intercepter tous les trafics qu'il désir.

Le schéma ci-dessous montre le procédé :



1 - Les cibles finales A et B s'échangent des informations normalement
2 - Le Switch est le maître du contexte Spanning Tree
3 - Le pirate Z envoi une trame BPDU avec un BID très faible
4 - Le commutateur admet que le pirate Z soit devenu le maître du contexte STP
5 - Le hacker redéfinis la topologie afin de rediriger les flux vers lui
6 - Les cibles A et B s'échangent des informations, mais le pirate les reçoit aussi

Ils existent plusieurs possibilités afin d'éviter cette attaque. Par exemple, il est possible :

- D'activer STP (Spanning Tree Protocol) uniquement sur les ports interconnectés à un autre commutateur
- D'activer STRG (Spanning Tree Root Guard) sur les commutateurs permettant de laisser passer les BPDU tant que le port en question ne demande pas à devenir maître dans l'instance Spanngin Tree.
- D'activer le BPDU Guard sur les Switchs afin de bloquer tous les types de message BPDU du port en question.

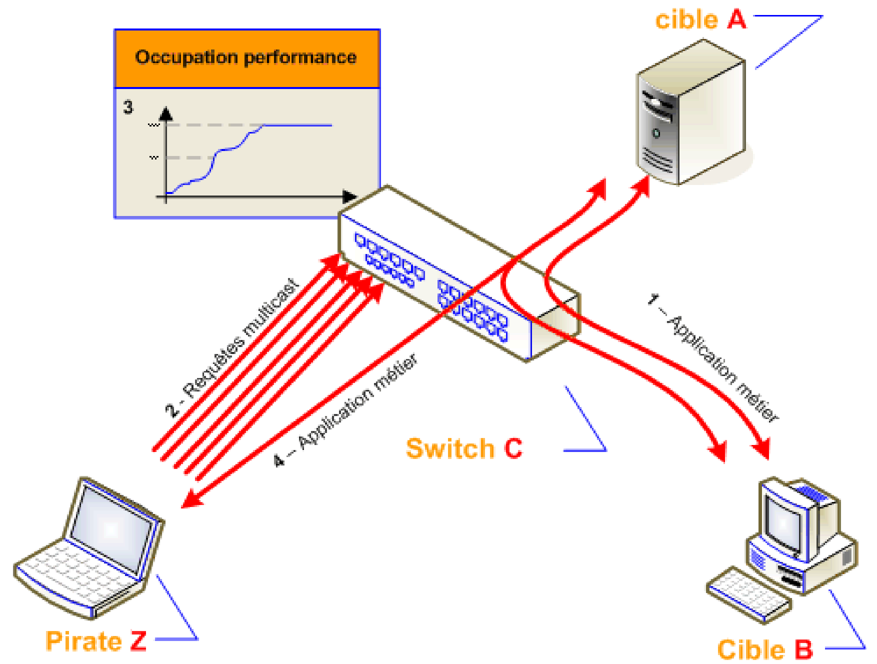
4. Attaque saturation processeur via BPDU

Cette attaque se base sur l'envoi massif de datagramme multicast (consommateur de processeur distant) à destination du Switch. L'intérêt est de changer le mode de fonctionnement du Switch afin qu'il travail en HUB. Cela est possible car certain Switch, à l'approche de la saturation processeur, préfère basculer en mode HUB afin de préserver une priorité sur l'exploitation.

Cela dépend du constructeur, de l'équipement et de la version, mais les conséquences peuvent être multiples comme par exemple :

- Buffer over flow du Switch (cette conséquence n'est plus réaliste de nos jours).
- Impossibilité au Switch de commuter la plus part des trames.
- Passage du Switch en mode HUB permettant ainsi à l'attaquant d'effectuer de l'écoute.

Le schéma ci-dessous montre le procédé :



1 - Les cibles finales A et B s'échangent des informations normalement
2 - Le pirate Z flood le Switch avec des requêtes Multicast
3 - Le Switch C voit son occupation processeur monter en flèche et bascule en mode HUB
4 - Les cibles A et B s'échangent des informations, mais le pirate les reçoit aussi

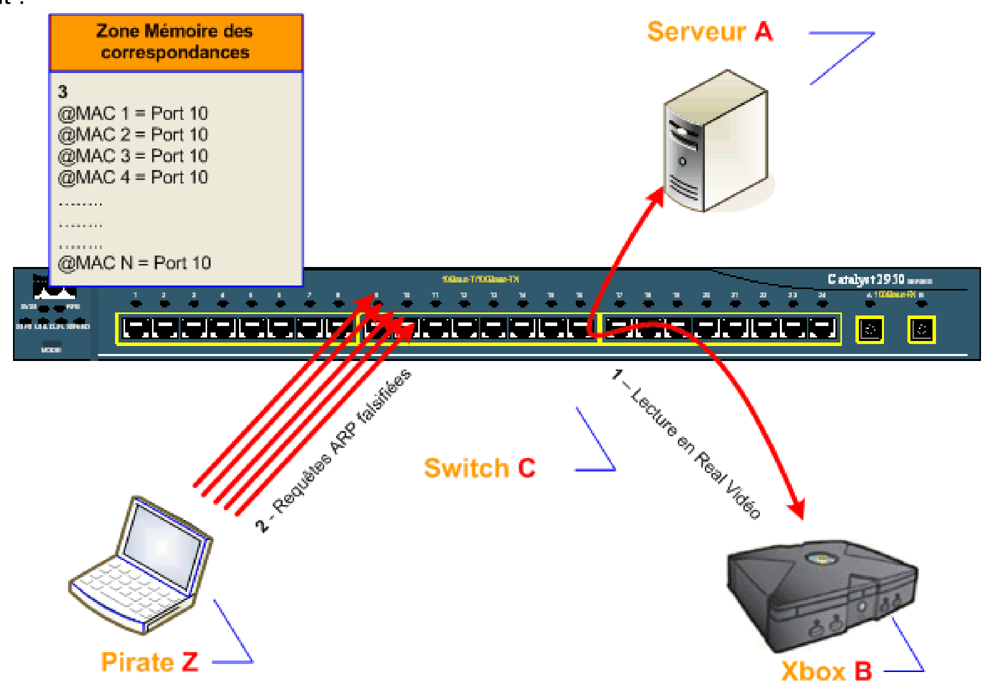
Ils existent plusieurs possibilités afin d'éviter cette attaque. Par exemple, il est possible :

- d'utiliser des Switchs travaillant en mode distribué apportant une gestion processeur décentralisé à chaque port
- d'applique un filtre IP sur chaque port afin d'éviter les requêtes à destination du Switch lui même

II. ETUDE DE L'ATTAQUE ARP POISONNING

1. Le contexte de l'attaque

Cette attaque consiste à saturer la mémoire du Switch qui contient la table d'adresses MAC. Cela peut être un Pirate, un utilisateur mal intentionné et voir même un Virus ou SpyWare. Pour réaliser cette attaque, on utilise le contexte suivant :

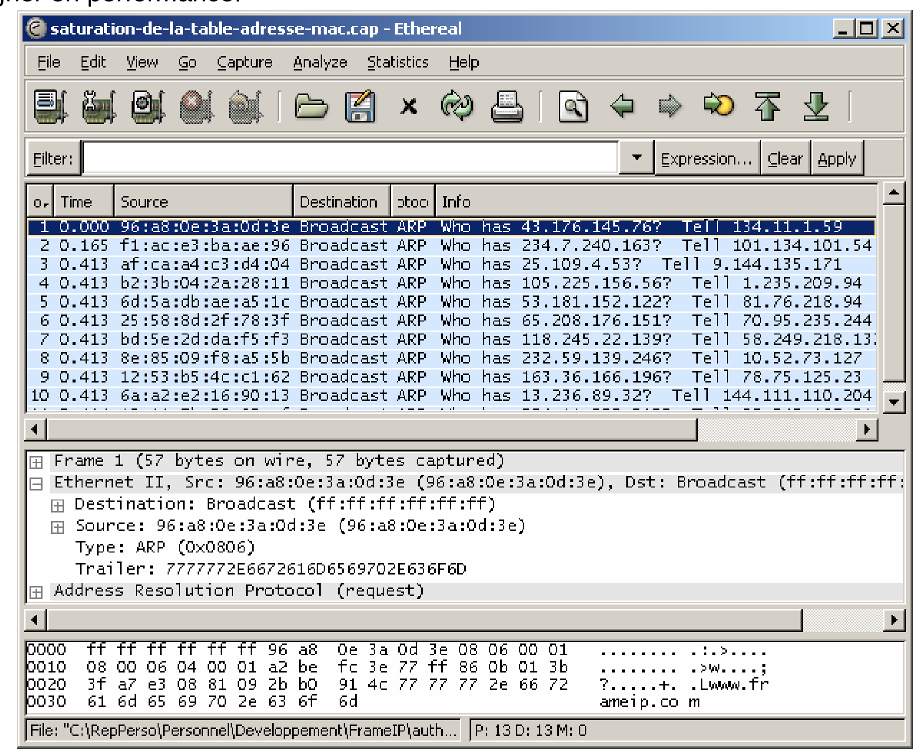


1 - La Xbox lit un film présent sur le serveur real vidéo.
2 - Le pirate envoi un flood de datagrammes avec une d'adresse MAC source aléatoire.
3 - Le Switch insert les adresses MAC dans sa table en les associant au port physique du port du pirate.

2. La réalisation

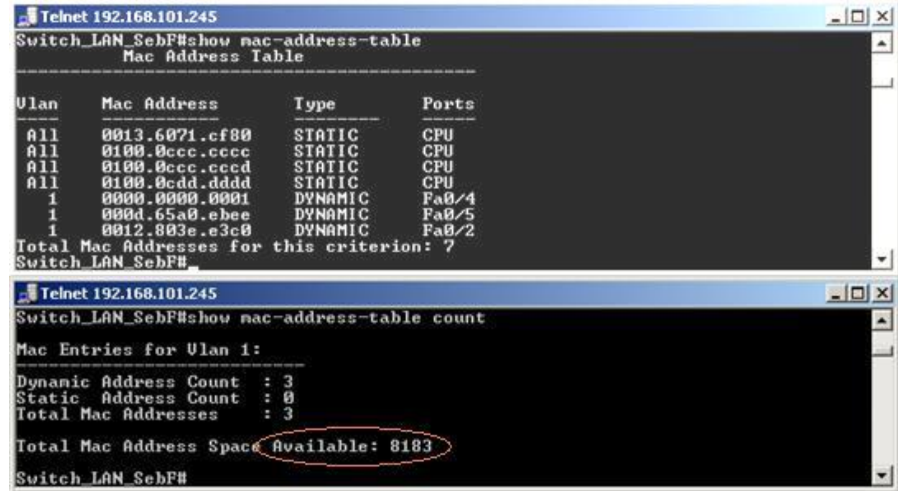
Pour réaliser cette attaque, on utilise la commande "arpflood.exe -interface 3 -loops 0 -view 0" qui permet l'envoi massif de requête ARP avec des adresses MAC aléatoires comme on peut le voir dans l'analyse de trame suivante.

On utilise les arguments "-loops 0" pour définir de ne pas s'arrêter et "-view 0" pour ne pas afficher les résultats à l'écran afin de gagner en performance.

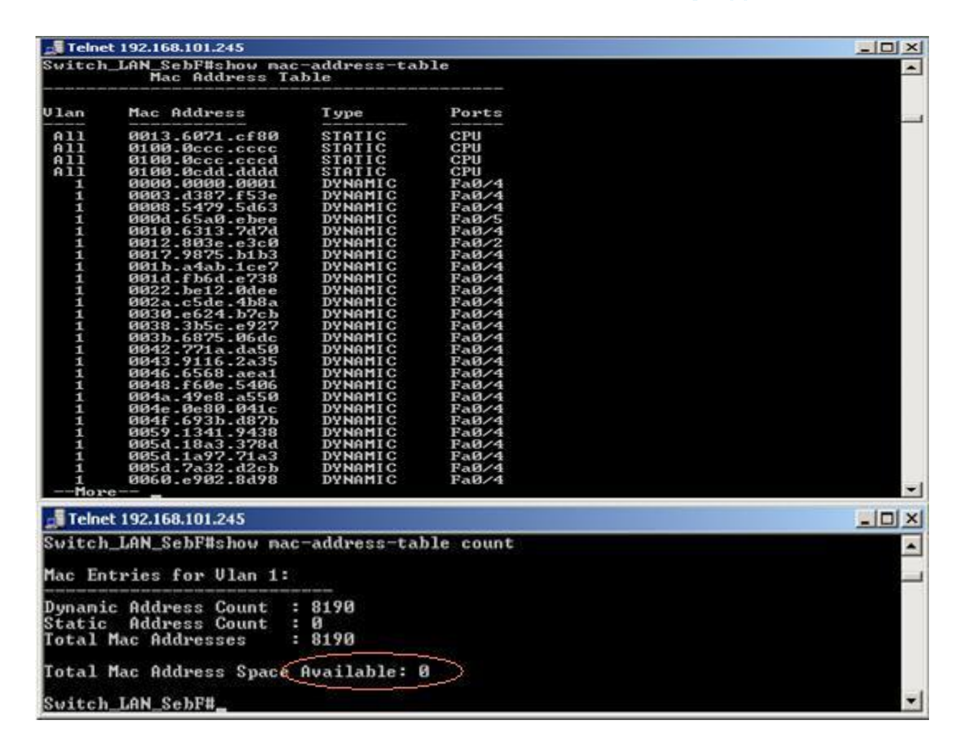


3. La réaction

La réaction du Switch est sans surprise : la table d'adresses MAC se remplie instantanément et sature très rapidement la mémoire. En fait, le Switch 2950 Cisco est limité à 8000 adresses MAC maximum. La commande ''show mac-address-table'' permet de voir la table des correspondances MAC. Voici le contenu à l'étape 1 :



Et après l'étape 2 (après l'exécution de Arpflood), on peut remarquer qu'il ne reste plus aucune place dans la table de correspondance :



4. Les conséquences

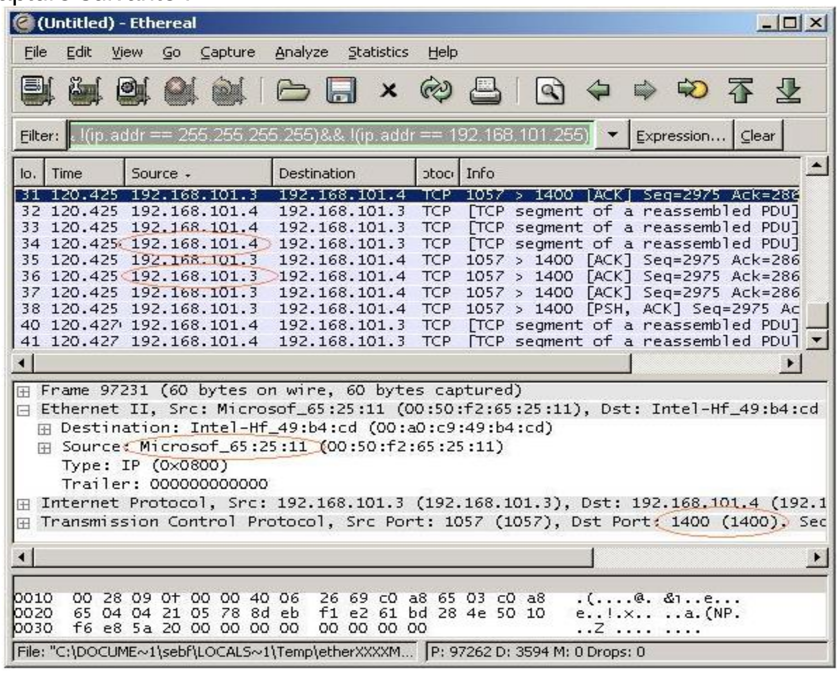
Il y a principalement deux conséquences visibles qui sont la perte de l'administration et le passage en mode HUB.

- Perte de l'administration

Dès les premières secondes de l'exécution du flooding ARP, le Switch répond très mal au management Telnet. L'affichage devient très lent et le temps de réponse à une commande est long. Cependant, le process de Throughput étant prioritaire, le Switch ne drop aucune trame à commuter, ce qui est une très bonne réaction. Cette première conséquence impact uniquement le management du Switch, mais aucunement sa fonction principale "la commutation".

- Passage en mode HUB

Par la suite, ne possédant plus de place pour stocker les correspondances des adresses MAC de la XBOX et du Serveur, le Switch est obligé de basculer en mode HUB. Ainsi, le Pirate Z peut alors écouter le flux real vidéo comme le montre la capture suivante :



En tant que pirate Z, mon PC portable reçoit donc l'ensemble du trafic échangé entre la XBOX 192.168.101.3 et le serveur 192.168.101.4. On remarque, en fait, que le passage en mode HUB du Switch peut intervenir de deux manières différentes :

- La première est le cas où le serveur et la XBOX ne discutent pas encore ensemble avant l'attaque. Le Switch ne connaît donc pas leurs adresses MAC. Ainsi, lorsque ArpFlood sature la table de correspondance, le Switch ne peut plus apprendre aucunes nouvelles adresses MAC. Dès que la XBOX et le serveur se mettent à discuter ensemble, le Switch renverra chacune des trames sur tous les ports du fait qu'il n'a pas placé leurs adresses MAC dans sa table de correspondance.
- La seconde manière est le cas où le serveur et la XBOX discutent ensemble avant l'attaque. Le Switch connaît donc leurs adresses MAC, même après l'exécution de ArpFlood. Le Switch commutera correctement le flux d'échange entre la XBOX et le serveur sur les ports concernés. A ce moment, l'écoute ne fonctionne pas. Il faut alors attendre 5 minutes, ce qui représente la durée de vie d'une entrée dans la table de correspondance, pour que le Switch commute le flux sur tous les ports. Car, au bout des 5 minutes, les correspondances MAC et Ports de la XBOX et du Serveur sont effacées et le Switch ne peut pas les réapprendre du fait que sa table est saturée.

Pour info, le Switch 2950 garde 5 minutes une correspondance d'adresse MAC/Port.

```
Telnet 192.168.101.245
Switch_LAN_SebF#sh mac-address-table aging-time vlan  1
Vlan    Aging Time
----    ----------
   1      300

Switch_LAN_SebF#_
```

Cela peut être redéfinit grâce à la commande "mac-address-table aging-time" commande dans l'exemple suivant où l'on positionne la durée de vie de l'entrée à 10 secondes :

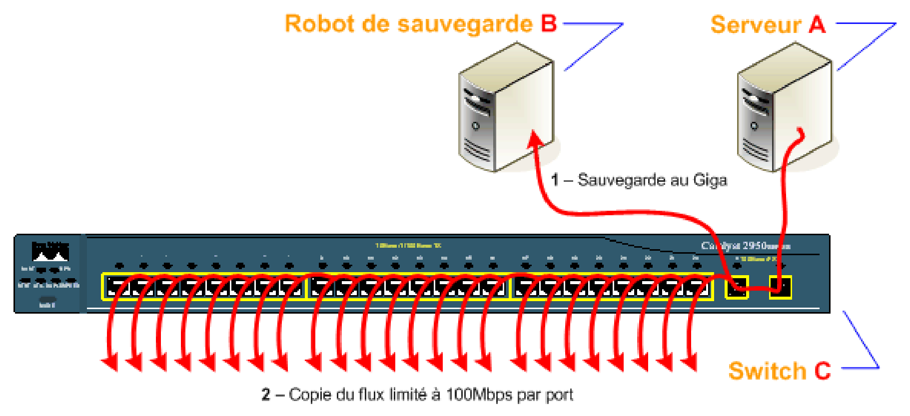
```
Telnet 192.168.101.245
Switch_LAN_SebF(config)#mac-address-table aging-time ?
  <0-0>          Enter 0 to disable aging
  <10-1000000>   Aging time in seconds

Switch_LAN_SebF(config)#mac-address-table aging-time 10
Switch_LAN_SebF(config)#exit
Switch_LAN_SebF#sh mac-address-table aging-time vlan 1
Vlan    Aging Time
----    ----------
   1      10

Switch_LAN_SebF#
```

<u>- Saturation réseau</u>

La conséquence suivante est que suite au passage en mode HUB, toutes les trames vont être multipliées sur tous les ports. Ainsi, si par exemple une sauvegarde au giga à lieu entre deux ports, le débit va se répliquer sur tous les autres ports en les saturants. L'incidence impacte alors chaque port du commutateur et donc les utilisateurs finaux.



De plus, un Switch possède un taux de commutation de fond de panier maximum. Par exemple, pour le Cisco Catalyst 2950T-24, la bande passante maximum de commutation globale est de 8,8 Gbps (8.8Gbps maximum forwarding bandwidth). Ainsi, avec la réplication des ports, on peut rapidement saturer la commutation globale du Switch. Le débit global est alors supérieur aux possibilités réelles du fond de panier.

5. Les protections non efficaces

- Augmenter la durée de vie des correspondances

L'une des possibilités est de diminuer la durée de vie des entrées de la table de correspondance. Cependant, cela ne permet pas de résoudre le problème, car si le pirate laisse tourner son flood, alors à peine libéré, le Switch apprendra de nouveau des adresses MAC spoofées.

- Acheter des commutateurs Ethernet plus performants

Etant donné que le Switch 2950 est limité à 8000 adresses MAC, l'idée étant d'acheter des commutateurs de gamme supérieure apportant donc de plus grandes de performances. Voici un tableau relatant les limites des différentes gammes Cisco :

Références	**Nombre d'@ MAX maximum**
Cisco Catalyst 2948 G-GE-TX	16000
Cisco Catalyst 3550-12G	12000
Cisco Catalyst 6500 Series	64000

On remarquera que chaque Switch possède de nouveau une limitation dans le nombre de correspondances. On peut donc prendre conscience que l'augmentation de la catégorie du Switch ne solutionne pas ce risque. Car on peut augmenter le nombre maximum de correspondances, cela ne change pas le fait que le hackeur va très rapidement saturer la mémoire de la table.

- Segmenter le commutateur par des VLAN

Même s'il est fortement recommandé d'utiliser les VLAN pour segmenter son réseau pour sécuriser son LAN, dans notre cas, cela n'apportera pas la protection nécessaire à la saturation de la table de correspondance.
En fait, dans le cas où j'ai deux VLAN (ou plus), la table de correspondance peut être lue indépendamment comme cela :



Cependant, si je flood de nouvelles adresses MAC dans un seul VLAN comme le 99, on remarque que la table de correspondance chute pour tous les VLAN. Cela montre bien que le nombre d'adresses MAC maximum par Switch est indépendante des VLAN.
Ainsi, la segmentation par VLAN ne résout pas le problème

6. Les protections efficaces

- Nombre d'adresses MAC maximum par port

La limitation d'un nombre maximal d'adresses MAC par port physique est une solution efficace. Elle permet ainsi de positionner le hacker dans un contexte isolé où il ne peut pas déborder sur la mémoire globale du Switch. Par exemple, si nous limitons chaque port à 100 adresses MAC maximum, cela permettra d'empêcher que le flood sature la mémoire globale du Switch. 100 paraît être une bonne valeur pour sécuriser les accès sans contraindre l'exploitation réseau de l'entreprise.

- Authentification 802.1X

L'activation 802.1X sur les ports, en plus d'apporter une bonne sécurité de votre LAN, vous permettra d'empêcher la saturation de la table de correspondance par un Hackeur ou un virus.

E . SÉCURISATION DES ROUTEURS CISCO

Les fonctionnalités d'un routeur font de lui un dispositif indispensable pour le fonctionnement d'un réseau de grande taille d'où l'importance de le protéger contre les attaques.

I. Définition de la politique de sécurité du routeur

1- Politique d'acquisition : il convient de définir les fonctionnalités qui seront assurées par le routeur ; quel constructeur offre le meilleur rapport qualité/prix ? Quel est la durée de la garantie ? Le support sera t-il assuré ? faut-il un contrat de maintenance ?

2- Politique de déploiement et de mise en service : cette politique devra tenir compte de son installation, de sa configuration et de sa mise en service. Par exemple, il doit être placé dans un endroit sécurisé (accès protégé), derrière un dispositif de protection comme un pare-feu par exemple. Il doit être testé avant sa mise en production. En cas de problème, on doit pouvoir revenir à la configuration de départ sans qu'il y ait d'impact sur le système d'information ou sur le réseau.

3- Politique des mots de passe Les routeurs offrent en général plusieurs types et niveaux d'accès (telnet, ligne virtuelle (vty), http, ligne auxiliaire, mode enable, mode de configuration globale, etc.). Chaque type d'accès peut être protégé par un mot de passe. Une politique des mots de passe doit être définie et appliquée pour éviter leur compromission. Par exemple, les mots de passe doivent être changés suivant une périodicité (tous les trois mois par exemple). Ils doivent être forts (difficillement cassable), c'est à dire composé des chiffres, caractères spéciaux (@§!&#), majuscules et minuscules. Ceci permet d'éviter les attaques par dictionnaire ou par force brute.

4- Politique de contrôle d'accès et d'exploitation : cette politique doit contenir des éléments sur la mise à jour de l'IOS, les droits et niveaux d'accès, les actions possibles en fonction des rôles, la périodicité des mises à jour des protocoles de routage, les routeurs voisins autorisés à communiquer avec le routeur…

5- Politique de durcissement : les services et comptes inutiles doivent être désactivé, les types d'accès autorisés doivent être bien définis ainsi que la politique de sauvegarde de la configuration, etc..

6- Politique de journalisation : il est important de surveiller un routeur afin d'avoir une idée sur ses différentes activités (trafic, connexion, etc.). Cette surveillance passe par les fichiers journaux générés par ce dernier.

II. Sécurisation des accès administratifs par mots de passe

1- Désactiver le service de réinitialisation des mots de passe Dans certains cas, il peut être nécessaire de désactiver le service qui permet de réinitialiser les mots de passe sur un routeur. Il est important de noter ici que cette désactivation peut avoir des conséquences graves, par exemple, l'obligation de revenir à la configuration par défaut de base (usine) du routeur.

R1(config)# no service passwords-recovery

En cas de perte de mot de passe, il sera impossible de réinitialiser le mot de passe du super utilisateur. Cette commande fait partie des commandes cachées de l'IOS Cisco. Je vous conseille de l'utiliser uniquement si vous n'avez pas une garantie suffisante au niveau de la maîtrise de l'accès physique de votre routeur.

2- Configurer la longueur minimale d'un mot de passe

R1(config)# security passwords min-length 10

Le routeur n'acceptera pas les mots de passe de moins de 10 caractères.

3- Limiter le nombre de tentatives de connexions échouées Afin d'éviter les attaques par dictionnaire et par force brute sur les mots de passe, il faut limiter le nombre de tentatives de connexions sans succès sur votre routeur (dans notre exemple, ce nombre est 4).

R1(config)# security authentication failure rate 4 log

Au bout de 4 tentatives de connexion sans succès en moins d'une minute, les informations seront enregistrées dans le journal des évènements.

R1(config)# login block-for 60 attempts 4 within 10

Au bout de 4 tentatives de connexion sans succès dans un intervalle de 10 seconde, une autre tentative ne sera possible qu'après 60 secondes, car le routeur restera silencieux pendant cette période.

Pendant cette periode, il sera impossible de se connecter sur le routeur. Ce qui pourrait affecter les administrateurs du routeur ayant les droits. Pour éviter cela, il faudra créer une ACL qui permet aux administrateurs de se connecter pendant cette période de silence (quiet-mode).

R1(config)# ip access-list standard login-permit-adm
R1(config-std-nac)# permit 172.16.20.0 0.0.0.255
R1(config)# exit
R1(config)# login quiet-mode access-class login-permit-adm

4- Empêcher les ouvertures de sessions sur les lignes (auxiliaires et virtuelles)

// Ligne auxiliaire
R1(config)# line aux 0
R1(config-line)# no password
R1(config-line)# login
R1(config-line)# exit

// Lignes virtuelle
R1(config)# line vty 0 4
R1(config-line)# no password
R1(config-line)# login
R1(config-line)# exit

5- Autoriser juste les accès distants en SSH (le telnet n'étant pas sécurisé)

R1(config)# line vty 0 4
R1(config-line)# no transport input
R1(config-line)# transport input ssh
R1(config-line)# exit

6- Configuration de la sécurité supplémentaire pour les lignes VTY, console et AUX

R1(config)# line vty 0 4
R1(config-line)# exec-timeout 5
R1(config-line)# exit
R1(config)# line console 0
R1(config-line)# exec-timeout 5
R1(config-line)# exit
R1(config)# line aux 0
R1(config-line)# exec-timeout 5
R1(config-line)# exit
R1(config)# service tcp-keepalives-in

7- Configuration de la sécurité SSH

R1(config)# hostname Ottawa // définition du nom d'hôte)
Ottawa(config)# ip domain-name cisco.com // définition du nom de domaine)
Ottawa(config)# crypto key generate rsa // génération des clés asymétriques
Ottawa(config)# username emabo secret cisco123
Ottawa(config)# line vty 0 4
Ottawa(config-line)# transport input ssh // configuration de l'authentification locale et VTY
Ottawa(config-line)# login local
Ottawa(config)# ip ssh time-out 10 // configuration des délais d'attente ssh
Ottawa(config)# ip ssh authentication-retries 3 // configuration des délais d'essai à nouveau ssh

8- Accorder une attention particulière aux vulnérabilités SNMP, NTP et DNS

Pour assurer ses fonctionnalités, un routeur s'appuie sur d'autres services comme comme le service de résolution des noms. Il se trouve que ces services sont souvent vulnérables. Il convient donc de s'assurer que les services auxiliaires sur lesquels s'appuie un routeur sont bien configurer et sécurisé.

9- Désactiver tous les services, protocoles et comptes inutiles

R1(config)# no service finger // exemple du service finger
R1(config)# no cdp run // exemple du protocole CDP

III. Sécurisation des protocoles de routages

Les protocoles de routages sont utilisés par un routeur pour mettre à jour dynamiquement, sa table de routage. Les informations de mise à jour circulant très souvent en clair entre les routeurs, il convient de configurer un minimum de sécurité pour ces protocoles. Cette partie du document qui se veut technique présente comment configurer certains protocoles de routage de manière sécurisé.

1- Configurer le protocole RIPv2 avec authentification

Ottawa(config)# router rip
Ottawa(config-router)# passive-interface default // désactivation de la propagation des mises à jour de routage
Ottawa(config-router)# no passive-interface serial 0/0 // activation de la propagation sur une seule interface
Ottawa(config)# key chain TOTO
Ottawa(config-keychain)# key 1
Ottawa(config-keychain-key)# key-string cisco
Ottawa(config)# interface serial 0/0
Ottawa(config-if)# ip rip authentication mode md5
Ottawa(config-if)# ip rip authentication key-chain TOTO

2- Configurer l'authentification du protocole de routage EIGRP

Ottawa(config)# key chain EIGRP_KEY
Ottawa(config-keychain)# key 1
Ottawa(config-keychain-key)# key-string CCNP
Ottawa(config)# interface serial 0/0
Ottawa(config-if)# ip authentication mode eigrp 1 md5
Ottawa(config-if)# ip authentication key-chain eigrp 1 EIGRP_KEY

3- Configurer l'authentification du protocole de routage OSPF

Ottawa(config)# interface serial 0/0
Ottawa(config-if)# ip ospf message-digest-key 1 md5 cisco
Ottawa(config-if)# ip ospf authentication message-digest
Ottawa(config-if)# exit
Ottawa(config)# router ospf 10
Ottawa(config-router)# area 0 authentication message-digest

4- Verrouiller le routeur à l'aide de Cisco "autosecure" "auto secure" est une commande créée par Cisco pour faciliter l'activation et la désactivation des services sur un routeur Cisco. Elle fonctionne en deux modes: interactive et non interactive

Ottawa# auto secure

Pour en savoir plus sur les fonctions exécutées par la commande "auto secure", je vous recommande ce site: http://www.ciscozine.com/2008/09/13/using-autosecure-to-secure-a-router/

IV. Configuration d'un routeur pour l'utilisation de SDM

SDM (Security Device Manager) est un outil permettant d'administrer des équipements (routeurs, commutateurs, etc.) via une interface graphique. La procédure permettant de configurer un routeur de manière à ce qui soit administrable par SDM est la suivante :

Ottawa#config t
Ottawa(config)# ip http server
Ottawa(config)# ip http secure-server
Ottawa(config)# ip http authentication local
Ottawa(config)# username emabo privilege 15 secret toto
R1(config)# line vty 0 4
R1(config-line)# privilege level 15
R1(config-line)# login local
R1(config-line)# transport input ssh

G . PRÉSENTATION ET CONFIGURATION D'AAA

1. Fonctionnalité d'AAA

AAA ou triple-A est une méthode modulaire qui s'articule autour de 3 points :

- L'authentification : fournir une méthode pour valider l'identité des utilisateurs, comme par exemple le couple login/mot de passe, le chalenge réponse (comme CHAP) ou encore les mots de passe à usage unique (One Time Password)
- L'autorisation : contrôler à quel équipement ou service l'utilisateur accrédité a accès, à quelle zone du réseau il peut se connecter, etc…
- Le comptage (accounting) : pouvoir quantifier et qualifier les actions des utilisateurs authentifiés, à des fins de facturation ou d'audit par exemple.

2. L'intérêt d'AAA dans la gestion des équipements

Au fur et à mesure de la croissance des réseaux, une administration individuelle de chaque ressource commence à devenir sérieusement lourde, sans parler des risques d'erreur de configuration liés à la répétition des procédures. Un simple mot de passe à changer devient un travail colossal à lui seul...

L'intérêt d'AAA est qu'il permet un fonctionnement sur un modèle client-serveur, lequel résout par construction même les problématiques de répétition de configuration sur chaque équipement individuellement.

Les équipements possèdent donc un client AAA, qui va récupérer les informations de connexion saisies par l'utilisateur par exemple, et les transmettre à son serveur AAA par l'intermédiaire de protocoles, tels que RADIUS ou TACACS+ que nous allons détailler plus loin.

Le serveur, quant à lui, sera en charge de valider l'identité de l'utilisateur, en vérifiant les informations fournies avec sa base d'identifiants. En cas de validité des informations, le serveur va transmettre l'information positive au client, ainsi que les autorisations dont il dispose. Sinon, il notifiera le client que l'authentification a échoué.

De cette manière, le serveur est capable de traiter la problématique AAA de manière centralisée, pour tous les équipements du réseau.

Comme vous pouvez vous en douter, le travail de l'administrateur sera grandement facilité. Un changement de mot de passe sur le serveur pour un utilisateur aura immédiatement une portée sur tous les équipements du réseau, sans avoir à les reconfigurer individuellement.

3. Les protocoles AAA

Les deux protocoles approuvés pour la communication entre un client et un serveur AAA sont RADIUS et TACACS+.

Je vous propose d'étudier leurs spécificités et leurs différences plus en avant, de manière à cerner celui qui convient le mieux à votre besoin.

3.1. RADIUS

Le protocole RADIUS a été mis au point par Livingston Enterprises Inc (Lucent) et il est implémenté par de nombreux constructeurs de serveur d'accès. Il est utilisé par de nombreuses entreprises, notamment des fournisseurs d'accès et il est aujourd'hui considéré comme le standard pour supporter AAA.

Ce protocole s'appuie sur UDP (protocole de transmission de données sans connexion et sans mécanismes de fiabilité de transmission) pour transmettre les données sur le réseau.

Il combine les services d'authentification et d'autorisation.

Il souffre de quelques problèmes, telle qu'une limitation de l'encryption des mots de passe à 16 bits ou encore des problèmes de disponibilité ou de timeout sur les périphériques, lorsqu'ils tentent de contacter le serveur.

Il est généralement utilisé pour l'accès aux réseaux, par PPP ou VPN notamment.

3.2. TACACS+

Le protocole TACACS+ a été mis au point par CISCO et c'est une amélioration des protocoles TACACS et Enhanced TACACS.

Il s'appuie sur TCP (protocole de transmission de données fiable, basé sur une connexion) pour véhiculer les données et crypte l'intégralité des informations avant leur transmission sur le réseau.

Ce protocole combine l'authentification, l'autorisation et l'accounting.

Il est généralement recommandé pour l'accès aux équipements.

4. Fonctionnalités détaillées d'ACS

4.1. Introduction

Cisco Secure Access Control Server (ACS) est une solution éditée par CISCO, permettant de traiter de manière centralisée les problématiques d'authentification, d'autorisation et de métrologie (Authentification Authorization Accounting) au sein d'un réseau. C'est un composant essentiel des services réseaux basés sur l'identité (IBNS ou Identity Based Networking Services) tels que les imagine l'éditeur.
Ce système fonctionne comme un système RADIUS ou TACACS+ et peut être utilisé pour gérer les accès à un grand nombre d'équipements réseau, tels que les routeurs, les réseaux privés virtuels (VPN), les pare feux, les commutateurs et les réseaux virtuels (VLAN), la voix IP ou encore les solutions sans fil.
Depuis la version 3.2, ACS est disponible en 2 versions :

- Un logiciel pour plateforme Windows Server
- Une version appliance 1U (Cisco Secure ACS Solution Engine)

4.2. Intégration globale d'ACS dans le réseau

ACS est un serveur de contrôle très fiable et performant, qui travaille comme un serveur RADIUS ou TACACS+ pour traiter les problématiques d'authentification, d'autorisation et de comptage pour les utilisateurs de ressources de l'entreprise au travers du réseau.
Il est administrable au travers d'une interface graphique et peut procurer la maîtrise AAA pour des milliers d'utilisateurs.
Il permet de gérer les règles d'accès utilisateur sur les IOS de routeurs, de PABX, de passerelles DSL, de pare feu, de serveur VPN, de bornes WIFI, de switch 802.1X, etc…

4.2.1. Fonctionnalités en termes d'authentification

Le couple traditionnel login/mot de passe est une méthode d'authentification qui est toujours supportée par ACS, bien qu'elle présente des risques qu'il ne faut pas ignorer, notamment si les droits accordés sont élevés.
Le mot de passe est crypté entre le client AAA et le serveur, quelque soit le protocole choisi (RADIUS ou TACACS+). Cependant, il circule en clair entre le poste utilisateur et le client AAA, ce qui peut constituer un risque.
Des méthodes d'authentification modernes existent pour s'affranchir de nombreux risques liés au couple login/mot de passe utilisé seul.
ACS en supporte un grand nombre, dont voici quelques exemples :

- CHAP (Challenge Handshake Authentication Protocol) : ce protocole est basé sur un challenge/réponse et permet à ACS de négocier la méthode la plus sécurisée que le client supporte pour communiquer. Le mot de passe est crypté durant tout le procédé.
- ARAP (Apple Remote Access Protocol) : le client final et le client AAA s'authentifient mutuellement avant de transmettre sur la base d'un challenge/réponse.
- LEAP (Lightweight Extensible Authentication Protocol) : basé sur un renouvellement dynamique de la clé WEP utilisée pour communiquer entre les équipements sans fils, il s'appuie sur les spécifications de 802.1X

ACS peut travailler sur une base de mots de passe externe, aussi bien que sur sa propre base.

4.2.2. Fonctionnalités en termes d'autorisation

Dès que l'utilisateur a été authentifié, le serveur ACS va envoyer le profil de l'utilisateur au client AAA, indiquant à quels services réseaux l'utilisateur a accès.
Il est possible de définir des règles d'accès par utilisateur ou par groupe, avec une granularité par période de temps, par service ou par niveau de sécurité.
Il sera ainsi possible d'interdire l'utilisation du service FTP durant une certaine période de la semaine (heures non ouvrées par exemple), pour prévenir les transferts de fichier à but non professionnel.
ACS permet également la désactivation de compte au-delà d'un certain nombre de tentatives de connexion ou l'expiration d'un compte au-delà d'une date donnée.
Enfin, il est possible de limiter le nombre de sessions simultanées par utilisateur ou groupe.

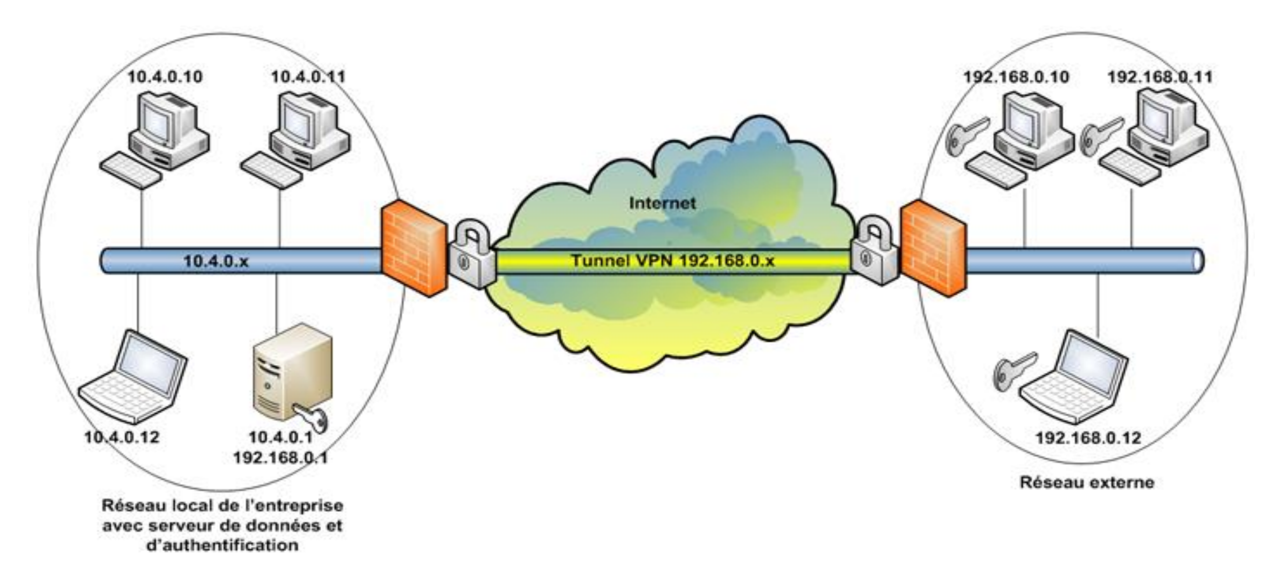
4.2.3. Fonctionnalités en termes de comptage

Une fois que l'utilisateur est authentifié et qu'il bénéficie de certains privilèges, le client AAA va pouvoir remonter des informations de métrologie au serveur ACS.
Ces informations peuvent être stockées sous forme de fichier CSV (Comma Separated Value – séparation des informations par une virgule) ou dans une base de données ODBC **(**Open Database Connectivity).
Le client peut remonter des informations telles que l'heure de début et de fin d'une session, la durée de la session, le nom de l'utilisateur établissant cette session, …
L'export et l'analyse de ces données permet la réalisation d'audits de sécurité ou de factures par exemple.

H. LES RESEAUX VPN

I. NOTIONS SUR LES RESEAUX VPN (Virtual Private Network)

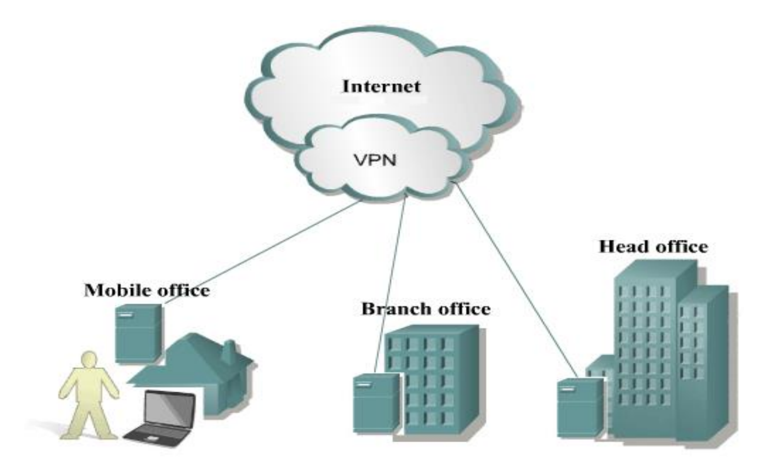
Un VPN (réseau privé virtuel) a pour fonction de faire abstraction des distances et de relier de façon sécurisée à travers Internet les différentes entités d'une entreprise. Ces entités peuvent être des établissements (siège social, agence, dépôts, usines…), des collaborateurs itinérants (nomades) ou travaillant à domicile (télé-travailleurs). Elles peuvent être également des utilisateurs ne faisant pas partie de l'entreprise (partenaires, fournisseurs, clients etc…), étant autorisés à accéder à certaines ressources.



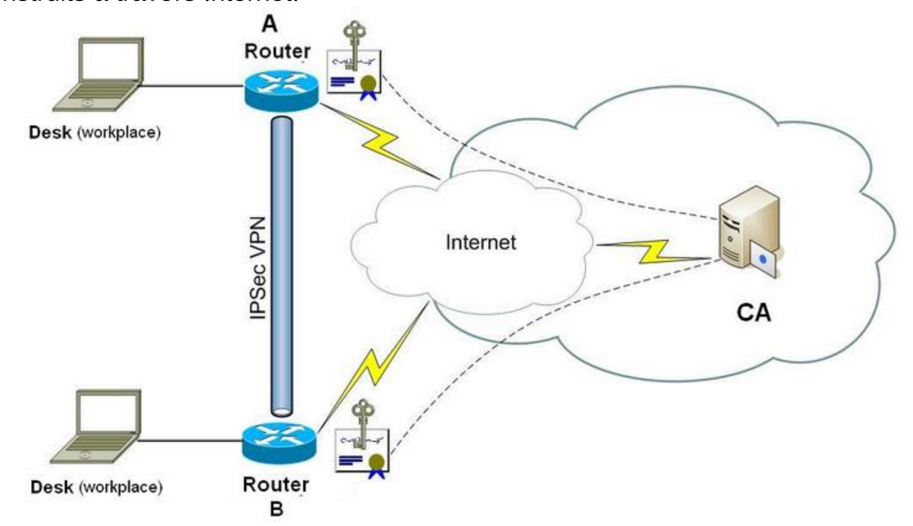
Concrètement, grâce au VPN, les utilisateurs peuvent utiliser, à distance et dans un environnement sécurisé, les logiciels métiers ou les documents, qui sont installés sur le serveur de l'entreprise.

- La sécurité des VPN repose sur la mise en place de 2 systèmes :
  - l'authentification, qui autorise les 2 entités à communiquer entre elles après avoir été identifiées ;
  - et le cryptage, qui rend indéchiffrable les informations échangées à travers Internet, afin qu'elles ne puissent être ni récupérées, ni lues par une personne étrangère à l'entreprise.

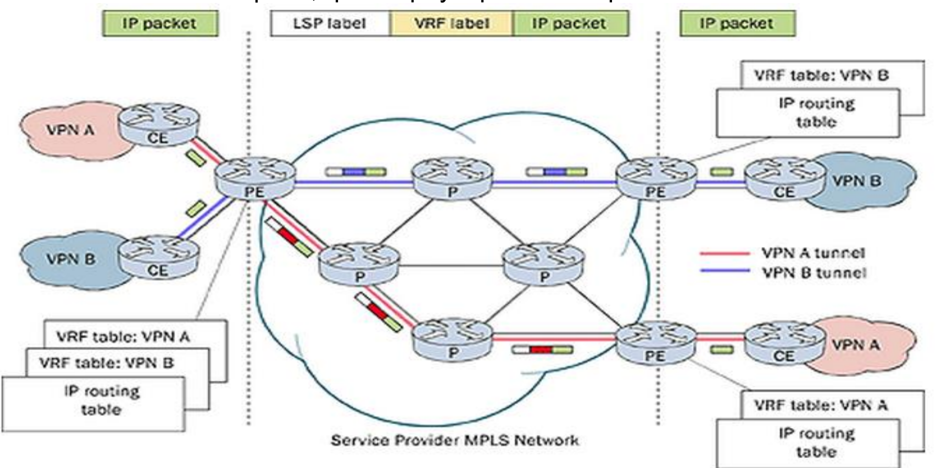
- Les architectures VPN sont de 3 types :
  - le VPN intranet qui permet de connecter de façon permanente les différents établissements de l'entreprise ou les télétravailleurs avec le site principal.
  - le VPN nomade qui est une extension du VPN Intranet. Il permet de connecter les utilisateurs nomades aux bureaux de l'entreprise.
  - et le VPN extranet qui est aussi une extension du VPN intranet. Il permet de connecter les utilisateurs ne faisant pas partie de l'entreprise (partenaires, fournisseurs, clients…).



- Les technologies VPN les plus utilisées sont de 3 types :
  - Le VPN IPSEC (Internet Protocol Security) repose sur la création de tunnels de communication cryptés et étanches construits à travers Internet.

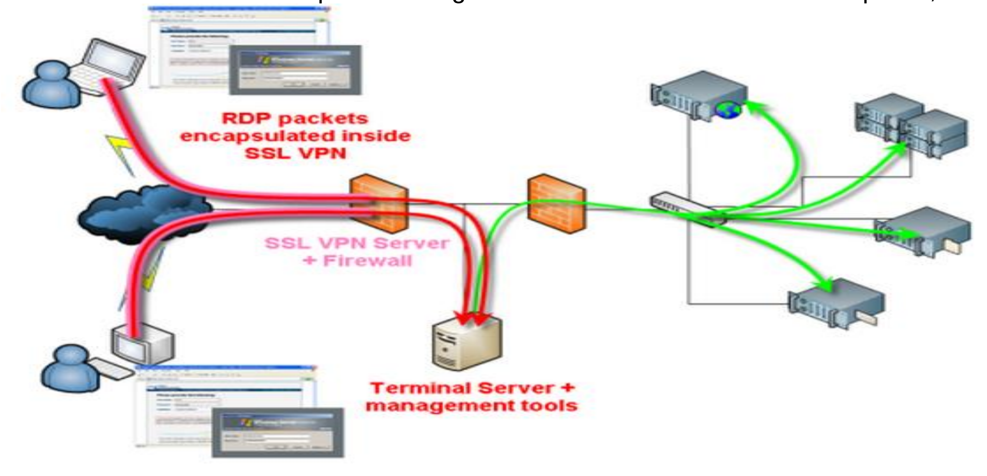


  - Le VPN MPLS (Multi Protocol Label Switching) repose sur la création de tunnels de communication étanches construits à travers le réseau privé du fournisseur d'accès à Internet. Ce dernier maîtrise, gère et sécurise entièrement son réseau privé, qui est physiquement séparé de l'Internet.



(VRF) Virtual Routing and Forwarding
(LSP) Label Switched Path

  - Le VPN SSL (Secure Sockets Layer) permet l'accès sécurisé, à travers Internet, aux logiciels métiers sans accéder au reste du réseau interne de l'entreprise. Cette technologie implique que les applications métiers soient webisées c.à.d. accessibles par les navigateurs Internet comme Internet Explorer, Firefox ou Opéra.



II. Les différentes méthodes de cryptographie

La cryptographie est une des disciplines de la cryptologie, s'attachant à protéger des messages (assurant confidentialité et/ou authenticité), en s'aidant souvent de secrets ou clés.
Elle est utilisée depuis l'antiquité, mais certaines de ses méthodes les plus importantes, comme la cryptographie asymétrique, n'ont que quelques dizaines d'années d'existence.

Vocabulaire

- chiffrement : le chiffrement est la transformation à l'aide d'une clé de chiffrement d'un message en clair en un message incompréhensible si on ne dispose pas d'une clé de déchiffrement
- chiffre : anciennement code secret, par extension, algorithme utilisé pour le chiffrement
- cryptogramme : message chiffré
- décrypter : déchiffrer c'est-à-dire retrouver le message clair correspondant à un message chiffré sans posséder la clé de déchiffrement ou même retrouver la clé de déchiffrement.
- cryptographie : étymologiquement écriture secrète, est devenue par extension l'étude de cet art. C'est donc aujourd'hui la science visant à créer des chiffres
- cryptanalyse : science analysant les cryptogrammes en vue de les casser
- cryptologie : science regroupant la cryptographie et la cryptanalyse.

1. Algorithmes de chiffrement faibles (cassables facilement)

Les premiers algorithmes utilisés pour le chiffrement d'une information étaient assez rudimentaires dans leur ensemble. Ils consistaient notamment au remplacement de caractères par d'autres. La confidentialité de l'algorithme de chiffrement est donc la pierre angulaire de ce système pour éviter un cassage rapide.

On distingue plusieurs méthodes de cryptanalyse :

Le chiffrement par substitution

On distingue généralement plusieurs types de cryptosystèmes par substitution:

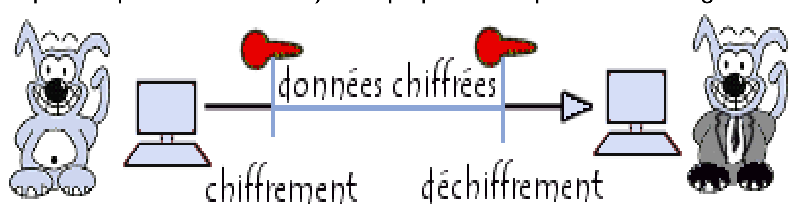
- La **substitution monoalphabétique** consiste à remplacer chaque lettre du message par une autre lettre.
- La **substitution homophonique** permet de faire correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères
- La **substitution de polygrammes** consiste à remplacer un groupe de caractères (polygramme) dans le message par un autre groupe de caractères

Le chiffrement de César

Ce code de chiffrement est un des plus anciens, dans la mesure où Jules César l'aurait utilisé. Le principe de codage repose sur l'ajout d'une valeur constante à l'ensemble des caractères du message.
Il s'agit donc simplement de décaler l'ensemble des valeurs des caractères du message d'un certain nombre de positions, c'est-à-dire en quelque sorte de substituer chaque lettre par une autre. Par exemple, en décalant le message "*COMMENT CA MARCHE*" de 3 positions, on obtient "*FRPPHQW FD PDUFKH*".
On appelle clé le caractère correspondant à la valeur que l'on ajoute au message pour effectuer le cryptage. Dans notre cas la clé est C, car c'est la 3ème lettre de l'alphabet.

2. Algorithmes de cryptographie symétrique (à clé secrète)

Les algorithmes de chiffrement symétrique se basent sur une même clé (ou presque) pour chiffrer et déchiffrer un message. Le problème de cette technique est qu'il faut que toutes les clés soient parfaitement confidentielles. Et lorsqu'un grand nombre de personnes désirent communiquer ensemble, le nombre de clés augmente de façon importante (une pour chaque couple communicant). Ce qui pose des problèmes de gestions des clés.



Quelques algorithmes de chiffrement symétrique très utilisés :

- DES (Data_encryption_standard) 3DES triple DES.
- AES (Advanced encryption standard) : Standard de chiffrement avancé.
- RC4 ; RC5 et d'autres.

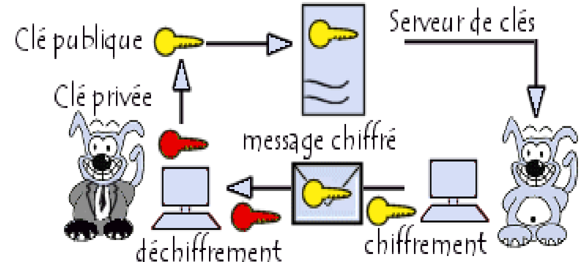
3. Algorithmes de cryptographie asymétrique (à clé publique et privée)

Pour résoudre en partie le problème de la gestion des clés, la cryptographie asymétrique a été mise au point dans les années 1970. Elle se base sur le principe de deux clés :

- une **publique**, permettant le chiffrement
- une **privée**, permettant le déchiffrement

Comme son nom l'indique, la clé publique est mise à la disposition de quiconque désire chiffrer un message. Ce dernier ne pourra être déchiffré qu'avec la clé privée, qui elle doit être confidentielle.

Ainsi, dans un système de chiffrement à clé publique, les utilisateurs choisissent une clé aléatoire qu'ils sont seuls à connaître (il s'agit de la *clé privée*). A partir de cette clé, ils déduisent chacun automatiquement un algorithme (il s'agit de la clé publique). Les utilisateurs s'échangent cette clé publique au travers d'un canal non sécurisé.



Lorsqu'un utilisateur désire envoyer un message à un autre utilisateur, il lui suffit de chiffrer le message à envoyer au moyen de la clé publique du destinataire (qu'il trouvera par exemple dans un serveur de clés tel qu'un annuaire LDAP (*Lightweight Directory Access Protocol*)).
Le destinataire sera en mesure de déchiffrer le message à l'aide de sa clé privée (qu'il est seul à connaître).

A titre d'image, il s'agit pour un utilisateur de créer aléatoirement une petite clé en métal (la clé privée), puis de fabriquer un grand nombre de cadenas (clé publique) qu'il dispose dans un casier accessible à tous (le casier joue le rôle de canal non sécurisé). Pour lui faire parvenir un document, chaque utilisateur peut prendre un cadenas (ouvert), fermer une valisette contenant le document grâce à ce cadenas, puis envoyer la valisette au propriétaire de la clé publique (le propriétaire du cadenas). Seul le propriétaire sera alors en mesure d'ouvrir la valisette avec sa clé privée.

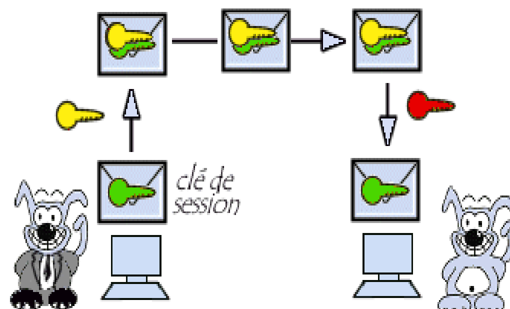
Avantages et inconvénients

Le problème consistant à se communiquer la clé de déchiffrement n'existe plus, dans la mesure où les clés publiques peuvent être envoyées librement. Le chiffrement par clés publiques permet donc à des personnes d'échanger des messages chiffrés sans pour autant posséder de secret en commun.

En contrepartie, toute la difficulté consiste à (s')assurer que la clé publique que l'on récupère est bien celle de la personne à qui l'on souhaite faire parvenir l'information chiffrée !

Intérêt d'une clé de session

Les algorithmes asymétriques (entrant en jeu dans les cryptosystèmes à clé publique) permettent de s'affranchir de problèmes liés à l'échange de clé via un canal sécurisé. Toutefois, ces derniers restent beaucoup moins efficaces (en terme de temps de calcul) que les algorithmes symétriques.



Ainsi, la notion de clé de session est un compromis entre le chiffrement symétrique et asymétrique permettant de combiner les deux techniques.
Le principe de la clé de session est simple : il consiste à générer aléatoirement une clé de session de taille raisonnable, et de chiffrer celle-ci à l'aide d'un algorithme de chiffrement à clef publique (plus exactement à l'aide de la clé publique du destinataire).

Le destinataire est en mesure de déchiffrer la clé de session à l'aide de sa clé privée. Ainsi, expéditeur et destinataires sont en possession d'une clé commune dont ils sont seuls connaisseurs. Il leur est alors possible de s'envoyer des documents chiffrés à l'aide d'un algorithme de chiffrement symétrique.

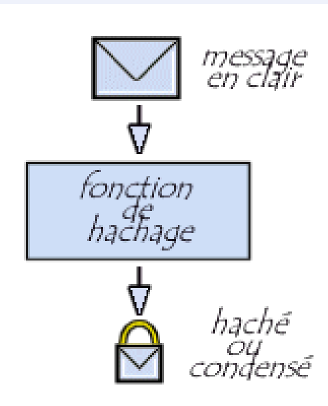
4. NOTIONS DE SIGNATURE ELECTRONIQUE

Le modèle de **signature électronique** (appelé aussi *signature numérique*) est un procédé permettant de garantir l'authenticité de l'expéditeur (fonction d'*authentification*) et de vérifier l'intégrité du message reçu.

La signature électronique assure également une fonction de non-répudiation, c'est-à-dire qu'elle permet d'assurer que l'expéditeur a bien envoyé le message (autrement dit elle empêche l'expéditeur de nier avoir expédié le message).

Qu'est-ce qu'une fonction de hachage ?

Une **fonction de hachage** (parfois appelée *fonction de condensation*) est une fonction permettant d'obtenir un condensé (appelé aussi *condensat* ou *haché* ou en anglais *message digest*) d'un texte, c'est-à-dire une suite de caractères assez courte représentant le texte qu'il condense. La fonction de hachage doit être telle qu'elle associe un et un seul haché à un texte en clair (cela signifie que la moindre modification du document entraîne la modification de son haché). D'autre part, il doit s'agir d'une fonction à sens unique (*one-way function*) afin qu'il soit impossible de retrouver le message original à partir du condensé. S'il existe un moyen de retrouver le message en clair à partir du haché, la fonction de hachage est dite « à brèche secrète ».



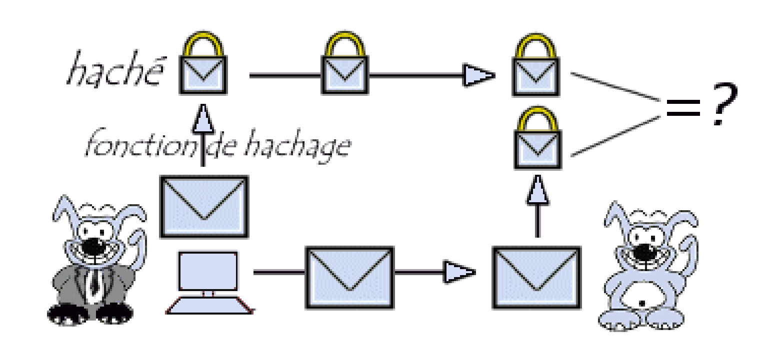
Ainsi, le haché représente en quelque sorte l'*empreinte digitale* (en anglais *finger print*) du document.

Les algorithmes de hachage les plus utilisés actuellement sont :

- **MD5** (*MD* signifiant *Message Digest*). Développé par Rivest en 1991, MD5 crée une empreinte digitale de 128 bits à partir d'un texte de taille arbitraire en le traitant par blocs de 512 bits. Il est courant de voir des documents en téléchargement sur Internet accompagnés d'un fichier MD5, il s'agit du condensé du document permettant de vérifier l'intégrité de ce dernier)
- **SHA** (pour *Secure Hash Algorithm*, pouvant être traduit par *Algorithme de hachage sécurisé*) crée des empreintes d'une longueur de 160 bits SHA-1 est une version améliorée de SHA datant de 1994 et produisant une empreinte de 160 bits à partir d'un message d'une longueur maximale de 2^{64} bits en le traitant par blocs de 512 bits.

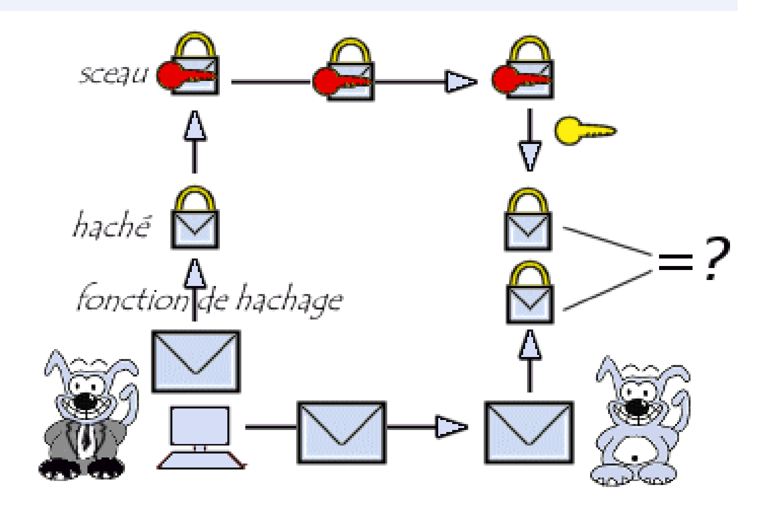
Vérification d'intégrité

En expédiant un message accompagné de son haché, il est possible de garantir l'intégrité d'un message, c'est-à-dire que le destinataire peut vérifier que le message n'a pas été altéré (intentionnellement ou de manière fortuite) durant la communication.



Lors de la réception du message, il suffit au destinataire de calculer le haché du message reçu et de le comparer avec le haché accompagnant le document. Si le message (ou le haché) a été falsifié durant la communication, les deux empreintes ne correspondront pas.

Le scellement des données



L'utilisation d'une fonction de hachage permet de vérifier que l'empreinte correspond bien au message reçu, mais rien ne prouve que le message a bien été envoyé par celui que l'on croit être l'expéditeur.

Ainsi, pour garantir l'authentification du message, il suffit à l'expéditeur de chiffrer (on dit généralement *signer*) le condensé à l'aide de sa clé privée (le *haché signé* est appelé **sceau**) et d'envoyer le sceau au destinataire.

A la réception du message, il suffit au destinataire de déchiffrer le sceau avec la clé publique de l'expéditeur, puis de comparer le haché obtenu avec la fonction de hachage au haché reçu en pièce jointe. Ce mécanisme de création de sceau est appelé *scellement*.

5. NOTIONS DE CERTIFICAT

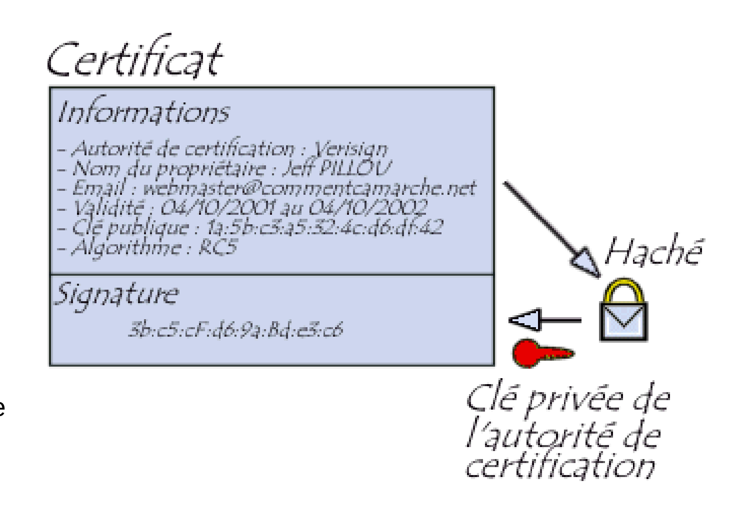
Les algorithmes de chiffrement asymétrique sont basés sur le partage entre les différents utilisateurs d'une clé publique. Généralement le partage de cette clé se fait au travers d'un annuaire électronique (généralement au format LDAP(Lightweight Directory Access Protocol)) ou bien d'un site web.

Toutefois ce mode de partage a une grande lacune : **rien ne garantit que la clé est bien celle de l'utilisateur a qui elle est associée**. En effet un pirate peut corrompre la clé publique présente dans l'annuaire en la remplaçant par sa clé publique. Ainsi, le pirate sera en mesure de déchiffrer tous les messages ayant été chiffrés avec la clé présente dans l'annuaire.

Ainsi un certificat permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé *autorité de certification* (souvent notée **CA** pour *Certification Authority*).

L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (équivalent à la date limite de péremption des produits alimentaires), ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).

Structure d'un certificat ?



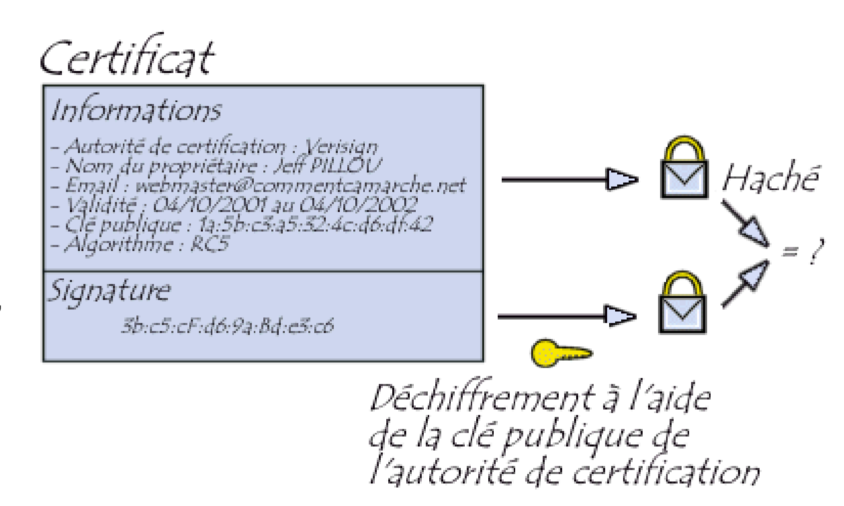
Les certificats sont des petits fichiers divisés en deux parties :

- La partie contenant les informations
- La partie contenant la signature de l'autorité de certification

La structure des certificats est normalisée par le standard **X.509** de l'UIT (plus exactement X.509v3), qui définit les informations contenues dans le certificat :

L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification, cela signifie qu'une fonction de hachage crée une empreinte de ces informations, puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification.

Lorsqu'un utilisateur désire communiquer avec une autre personne, il lui suffit de se procurer le certificat du destinataire. Ce certificat contient le nom du destinataire, ainsi que sa clé publique et est signé par l'autorité de certification. Il est donc possible de vérifier la validité du message en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat, en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière et en comparant ces deux résultats.



Signatures de certificats

On distingue différents types de certificats selon le niveau de signature :

- Les **certificats auto-signés** sont des certificats à usage interne. Signés par un serveur local, ce type de certificat permet de garantir la confidentialité des échanges au sein d'une organisation, par exemple pour le besoin d'un intranet. Il est ainsi possible d'effectuer une authentification des utilisateurs grâce à des certificats auto-signés.
- Les **certificats signés par un organisme de certification** sont nécessaires lorsqu'il s'agit d'assurer la sécurité des échanges avec des utilisateurs anonymes, par exemple dans le cas d'un site web sécurisé accessible au grand public. Le certificateur tiers permet d'assurer à l'utilisateur que le certificat appartient bien à l'organisation à laquelle il est déclaré appartenir.

III. Le protocole IPSec

1. Modes du protocole IPsec

IPSec est un protocole défini par l'IETF (Internet Engineering Task Force) permettant de sécuriser les échanges au niveau de la couche réseau. Il s'agit en fait d'un protocole apportant des améliorations au niveau de la sécurité au protocole IP afin de garantir la confidentialité, l'intégrité et l'authentification des échanges.
Il existe deux modes pour IPSec :

- ➢ le mode transport permet de protéger principalement les protocoles de niveaux supérieurs :
  - IPSec récupère les données venant de la couche 4 (TCP/transport), les signe et les crypte puis les envoie à la couche 3 (IP/réseau). Cela permet d'être transparent entre la couche TCP et la couche IP et du coup d'être relativement facile à mettre en place.
  - Il y a cependant plusieurs inconvénients :
    - o l'entête IP est produite par la couche IP et donc IPSec ne peut pas la contrôler dans ce cas.
    - o Il ne peut donc pas masquer les adresses pour faire croire à un réseau LAN virtuel entre les deux LAN reliés

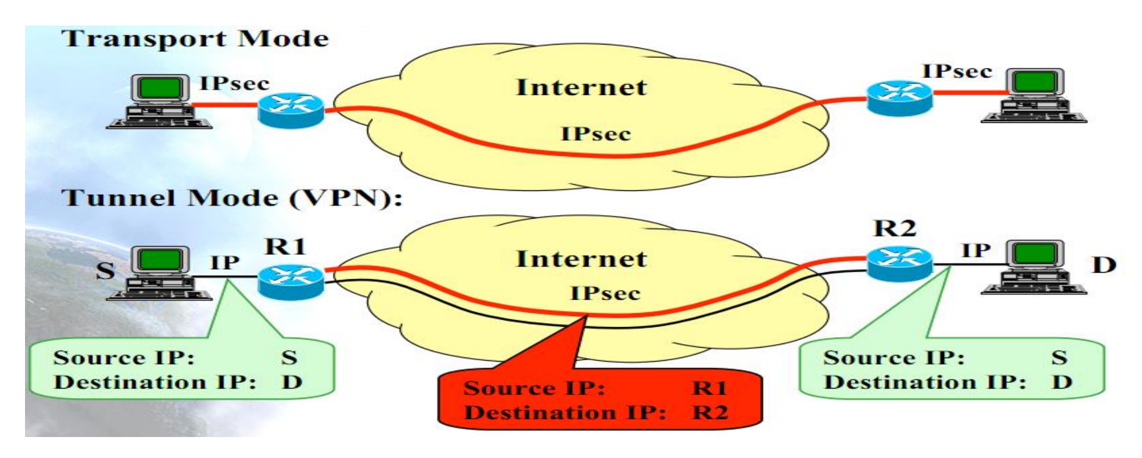


- ➢ le mode tunnel permet d'encapsuler des datagrammes IP dans des datagrammes IP
  - Les paquets descendent dans la pile jusqu'à la couche IP et c'est la couche IP qui passe ses données à la couche IPSec. Il y a donc une entête IP encapsulée dans les données IPSec et une entête IP réelle pour le transport sur Internet.
  - Cela a beaucoup d'avantages :

- l'entête IP réelle est produite par la couche IPSec. Cela permet d'encapsuler une entête IP avec des adresses relative au réseau virtuel et en plus de les crypter de façon à être sûr qu'elles ne sont pas modifiées.
- On a donc des adresses IP virtuelles donc tirant partie au mieux du concept de VPN
- On a le contrôle total sur l'entête IP produite par IPSec pour encapsuler ses données et son entête IPSec.



La figure suivante illustre la différence entre ces deux modes



2. Les composantes d'IPSec

Le protocole IPSec est basé sur trois modules :

- IP Authentification Header (AH) concernant l'intégrité, l'authentification et la protection contre le rejoue. des paquets à encapsuler
- Encapsulating Security Payload (ESP) définissant le chiffrement de paquets. ESP fournit la confidentialité, l'intégrité, l'authentification et la protection contre le rejoue.
- Security Assocation (SA) définissant l'échange des clés et des paramètres de sécurité. Les SA rassemblent ainsi l'ensemble des informations sur le traitement à appliquer aux paquets IP (les protocoles AH et/ou ESP, mode tunnel ou transport, les algorithmes de sécurité utilisés par les protocoles, les clés utilisées,...).

3. L'échange des clés

L'échange des clés nécessaires au cryptage des données dans IPSec peut se faire de deux façons différentes :

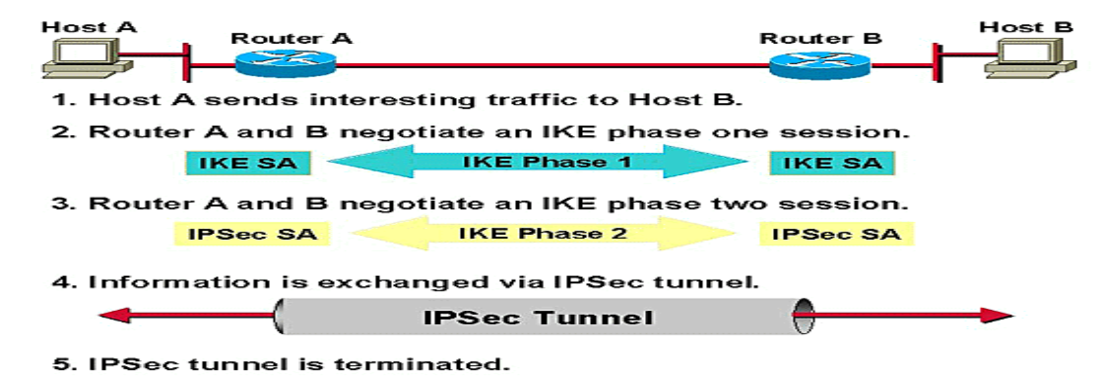
- à la main : pas très pratique
- IKE (Internet Key Exchange) : c'est un protocole développé pour IPSec. ISAKMP (Internet Security Association and Key Management Protocol) en est la base et a pour rôle la création (négociation et mise en place), la modification et la suppression des SA.

IV. Le protocole IKE et ses différentes phases

IKE est un protocole servant à IPSec et qui permet :

- Authentification des peers IPSec.
- Négociation des SA(Security Associations) IKE et IPsec.
- Etablissement des clés pour les algorithmes d'encryptions utilisés par IPSec.

IKE se déroule en deux phases :



- Phase 1 d'IKE

La phase 1 est connue sous le nom de Main Mode (mode principal). Pendant la phase 1, IKE utilise des méthodes de chiffrement de clé publique pour s'authentifier auprès d'entités IKE homologues. Il en résulte une association de sécurité (SA, security association) ISAKMP (Internet Security Association and Key Management Protocol). Une SA ISAKMP est un canal sécurisé sur lequel IKE négocie les numéros de clé des datagrammes IP. Contrairement aux SA IPsec, les SA ISAKMP sont bidirectionnelles. Il n'est donc pas nécessaire de disposer de plus d'une association de sécurité.

IKE Phase I for Security Gateways

GW1
GW2
Encryption methods/algorithms
- Peers exchange information on encryption methods/algorithms

GW1 Private Key
GW 1Public Key
GW2 Public Key
GW2 Private Key
- From a pool of random bits, each side produces a DH private key
- Each peer computes a DH public key from its private key

GW1 Private Key
GW2 Private Key
GW2 Public Key
GW 1Public Key
- Public keys are exchanged
- Each side produces a shared secret key from their private key and the other's public key.

Shared Secret Key (DH key)
Shared Secret Key (DH key)
- Shared secret key is the Diffie-Hellman key (DH Key)

ID, certificate
ID, certificate
- Peers exchange identities and certificates (encrypted data)

IKE SA

- Phase 2 d'IKE

La phase 2 est connue sous le nom de Quick Mode (mode rapide). Lors de la phase 2, IKE crée et gère les SA IPsec entre les systèmes qui exécutent le démon IKE. IKE utilise le canal sécurisé qui a été créé lors de la phase 1 pour protéger la transmission des numéros de clé. Le démon IKE crée les clés à partir d'un générateur de nombres aléatoires. Le démon actualise les clés à une fréquence qui peut être configurée.